

**THE GOVERNMENT OF
VIETNAM**

No. 330/2026/ND-CP

**SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness**

Hanoi, August 19, 2026

DECREE

PENALTIES FOR ADMINISTRATIVE VIOLATIONS IN FIELDS OF CYBERSECURITY AND PERSONAL DATA PROTECTION

Pursuant to the Law on Government Organization No. 63/2025/QH15;

Pursuant to the Law on Local Government Organization No. 72/2025/QH15;

*Pursuant to the Law on Promulgation of Legislative Documents No. 64/2025/QH15, amended by
Law No. 87/2025/QH15;*

Pursuant to the Law on Cybersecurity No. 116/2025/QH15;

Pursuant to the Law on Personal Data Protection No. 91/2025/QH15;

*Pursuant to the Law on Handling of Administrative Violations No. 15/2012/QH13, amended by
Law No. 54/2014/QH13, Law No. 18/2017/QH14, Law No. 67/2020/QH14, Law No.
09/2022/QH15, Law No. 11/2022/QH15, Law No. 56/2024/QH15, Law No. 88/2025/QH15, Law
No. 116/2025/QH15, and Law No. 120/2025/QH15;*

Pursuant to the Law on Digital Transformation No. 148/2025/QH15;

Pursuant to the Law on Electronic Transactions No. 20/2023/QH15;

Pursuant to the Law on Electronic Commerce No. 122/2025/QH15;

Pursuant to the Law on Digital Technology Industry No. 71/2025/QH15;

At the request of the Minister of Public Security of Vietnam;

*The Government of Vietnam hereby promulgates the Decree on penalties for administrative
violations in the fields of cybersecurity and personal data protection.*

Chapter I

GENERAL PROVISIONS

Article 1. Scope

1. This Decree provides for administrative violations; terminated administrative violations and ongoing administrative violations; penalties, penalty levels, and remedial measures applicable to each administrative violation; entities subject to penalties; sanctioning competence, specific maximum fine levels applicable to each title and competence to make written records of administrative violations; and the enforcement of penalties for administrative violations and remedial measures in each of the fields of cybersecurity and personal data protection.

2. Other administrative violations related to the fields of cybersecurity and personal data protection not prescribed in this Decree shall be sanctioned under relevant Decrees of the Government of Vietnam that prescribe penalties for administrative violations in the corresponding fields of state management.

3. Where an act concurrently violates this Decree and a decree prescribing penalties for administrative violations in another field of state management, the competent authority shall accurately determine the nature of the act and the applicable legal grounds for imposing a penalty. Where the act is concurrently prescribed in this Decree and in a decree prescribing penalties for administrative violations in another field of state management, this Decree shall apply if the violation is committed in the field of cybersecurity or personal data protection. Where the act contains constituent elements of a violation of obligations, responsibilities, or prohibitions falling within another specialized field of state management, the decree applicable to that field shall apply.

Article 2. Regulated entities and principles of application

1. Vietnamese individuals and organizations and foreign individuals and organizations committing administrative violations in the fields of cybersecurity and personal data protection within the territory, internal waters, territorial sea, contiguous zone, exclusive economic zone, or continental shelf of the Socialist Republic of Vietnam, or aboard aircraft of Vietnamese nationality or seagoing vessels flying the Vietnamese flag (hereinafter collectively referred to as “individuals and organizations”), except where otherwise prescribed by an international treaty to which the Socialist Republic of Vietnam is a contracting party.

2. Organizations prescribed in Clause 1 of this Article include:

a) Sole proprietorships, joint stock companies, limited liability companies, partnerships, and dependent units of enterprises;

b) Organizations established in accordance with the Law on Cooperatives;

c) Organizations established in accordance with the Law on Investment;

d) Socio-political organizations, socio-professional organizations, and other social organizations;

dd) Foreign enterprises or branches, representative offices, and business locations of foreign enterprises providing telecommunications services, Internet services, cyberspace content services, information technology services, cybersecurity services, or cross-border services; and

foreign agencies and organizations directly participating in or related to the processing of personal data of Vietnamese citizens and persons of Vietnamese origin whose nationality has not yet been determined, who reside in Vietnam and have been issued identity certificates;

e) Telecommunications service outlets, public electronic gaming service outlets, and public Internet access points;

g) Enterprises providing information content services on mobile telecommunications networks and in cyberspace;

h) Public service providers, social organizations, socio-professional organizations, and foreign non-governmental organizations using radio frequencies;

i) Domain name registrars and organizations or enterprises registering domain names;

k) Information system administrators and information system operators;

l) Other organizations as prescribed by law.

3. Business households, households, and residential communities committing administrative violations prescribed in this Decree shall be subject to the fine levels applicable to individual administrative violators.

4. The Ministry of National Defense shall exercise state management of cybersecurity in respect of military and national defense duties. The Ministry of Public Security of Vietnam shall, within its competence, exercise state management of cybersecurity in respect of military units engaged in civil or economic activities. For overlapping matters, if any, the Ministry of Public Security of Vietnam and the Ministry of National Defense of Vietnam shall agree upon cooperation regulations.

Article 3. Prescriptive period for imposing penalties for administrative violations

1. The prescriptive period for imposing penalties for administrative violations in the fields of cybersecurity and personal data protection shall be 1 year.

2. The time at which a violation terminates for the purpose of calculating the prescriptive period shall be the date on which the individual or organization completes the obligation prescribed by law or the date on which the violation actually terminates, as certified by the competent authority.

3. In addition to Clause 2 of this Article, authorities and persons competent to impose penalties for administrative violations shall rely on relevant legislative documents, dossiers, documents, and the circumstances of each specific case to determine whether a violation has terminated or remains ongoing in accordance with the current Decree of the Government of Vietnam elaborating on a number of articles of, and measures for implementing, the Law on Handling of Administrative Violations.

Article 4. Penalties

1. The principal penalties for administrative violations in the fields of cybersecurity and personal data protection include:

a) Warning;

b) Fine.

2. Depending on the nature and severity of the violation, an organization or individual committing an administrative violation may also be subject to one or more of the following additional penalties:

a) Deprivation of the right to use a license or practicing certificate for a definite period of between 1 and 24 months, including a license to provide social networking services; a license to establish a news aggregator site; a license to trade in cybersecurity products or services; a certificate of eligibility to provide personal data processing services; or a business license or practicing certificate for a business line or occupation involving a violation of regulations on personal data processing;

b) Suspension of operations for a definite period of between 1 and 24 months;

c) Confiscation of exhibits of administrative violations or means used for committing administrative violations (hereinafter collectively referred to as “exhibits and means of administrative violations”);

d) Expulsion of a foreigner committing an administrative violation.

3. The additional penalties prescribed in Clause 2 of this Article shall be imposed together with the principal penalty applicable to each specific violation prescribed in Chapter II of this Decree.

4. During the consideration and handling of a violation, if the violation is considered to show signs of a criminal offense, the transfer of the violation dossier for criminal prosecution, or the transfer of the violation dossier for the imposition of an administrative penalty where criminal prosecution is not pursued, shall comply with Articles 62 and 63 of the Law on Handling of Administrative Violations.

Article 5. Remedial measures

An individual or organization committing an administrative violation prescribed in this Decree shall be subject to one or more of the following remedial measures:

1. Mandatory restoration of the information system to its original state.

2. Mandatory recovery or return of information, data, programs, software, malware, digital accounts, digital certificates, products, equipment, services, Internet resources, domain names, IP

addresses, autonomous system numbers (ASNs), subscriber numbers, telecommunications numbering resources, tools, means, or other elements that violate the law on cybersecurity and the law on personal data protection.

3. Mandatory implementation of measures to remedy cybersecurity incidents, data disclosures or leaks, information conflicts in cyberspace, or risks of damage to agencies, organizations, or individuals; mandatory revocation of domain names involved in violations.

4. Mandatory removal of violating elements from the design, construction, management, or operation of information systems; personal data processing activities; technical processes; management mechanisms; service provision contracts; or data connection, retention, transmission, and sharing activities.

5. Mandatory correction of false or misleading information; correction of appraisal, assessment, inspection, or certification results; public notification or apology; or provision of complete and transparent information to organizations and individuals affected by the violation.

6. Mandatory implementation of necessary technical and managerial measures to prevent and remedy risks to cybersecurity or network safety caused by the violation; mandatory implementation of cybersecurity safeguards for information systems important to national security.

7. Mandatory full fulfillment of data subject rights; rectification, updating, supplementation, or deletion of personal data that is inaccurate or has been unlawfully collected, processed, used, publicly disclosed, or transferred.

8. Mandatory return or remittance of illegal profits obtained from administrative violations in the fields of cybersecurity and personal data protection.

9. Mandatory remittance of an amount equal to the value of exhibits or means of administrative violations that have been sold, dispersed, or unlawfully destroyed.

10. Mandatory re-inspection of the cybersecurity of products, equipment, services, and software used for protecting state secrets.

Article 6. Enforcement of penalties for administrative violations and remedial measures in each field of state management

1. Proceeds obtained from an administrative violation involving personal data protection as prescribed in this Decree comprise the entire value in kind, money, security instruments, assets, or other material benefits directly or indirectly obtained by an organization or individual from committing a violation of the law on personal data protection. Where an organization or individual commits multiple administrative violations or repeatedly commits an administrative violation, the proceeds obtained from the violation shall be determined separately for each administrative violation and each commission thereof.

2. Proceeds obtained from an administrative violation involving personal data protection shall be determined as follows:

a) For the unlawful purchase or sale of personal data, the proceeds shall be the total transaction value recorded in contracts, invoices, payment documents, message histories, electronic transactions, bank account statement data, electronic wallets, or other similar forms directly related to the transaction, without deducting any expenses incurred during the commission of the violation;

b) For the unlawful collection, processing, use, or transfer of personal data that does not involve the unlawful purchase or sale of personal data, the proceeds shall be the total actual revenue obtained by the violating organization or individual from business activities using the unlawfully collected, processed, used, or transferred personal data, without deducting any expenses incurred during the commission of the violation.

3. Organization of the enforcement of decisions on penalties for administrative violations and decisions on the application of remedial measures:

a) Violating individuals and organizations shall strictly and fully comply with decisions on penalties for administrative violations and decisions on the application of remedial measures within the time limits specified therein;

b) The person who issued the penalty decision or the authority to which the person competent to impose penalties belongs shall organize the enforcement of the decision and provide instructions to, and urge, violating individuals and organizations to fulfill their prescribed obligations;

c) Penalties and remedial measures shall be enforced in accordance with the Law on Handling of Administrative Violations and relevant laws, ensuring compliance with the prescribed procedures and the principles of transparency and objectivity, and ensuring timely enforcement.

4. Supervision and inspection of compliance:

a) Authorities and persons competent to impose penalties shall monitor and inspect the implementation of decisions on penalties and decisions on the application of remedial measures by violating individuals and organizations;

b) Where necessary, the competent authority may require a violating individual or organization to submit a written report and provide documents proving that the penalty decision or remedial measures have been fully complied with;

c) An inspection shall be documented in a written record or a document certifying the enforcement results, which shall be retained in the administrative violation case file.

5. Reporting on implementation results:

a) Violating individuals and organizations shall report on the results of implementing penalty decisions and decisions on the application of remedial measures at the request of the competent authority;

b) Authorities and persons competent to impose penalties shall compile statistics, consolidate information, and report on the results of enforcing decisions on penalties for administrative violations in accordance with the law.

6. Handling of non-compliance:

a) Where the enforcement period specified in a decision has expired, and the violating individual or organization fails to voluntarily comply with the decision, the decision shall be subject to mandatory enforcement in accordance with the Law on Handling of Administrative Violations;

b) An individual or organization that deliberately delays, evades, or obstructs the enforcement of a penalty decision or a decision on the application of remedial measures shall, depending on the nature and severity of the violation, be handled in accordance with the law;

c) The costs of organizing enforcement and compulsory enforcement shall be borne by the violating individual or organization in accordance with the law.

Article 7. Fine levels and sanctioning competence

1. Sections 1 through 5 of Chapter II of this Decree prescribe fine levels applicable to administrative violations committed by individuals in the field of cybersecurity. Where an organization commits the same violation, the fine applicable to the organization shall be twice the fine applicable to an individual.

Section 6 of Chapter II of this Decree prescribes fine levels applicable to administrative violations committed by organizations in the field of personal data protection. Where an individual commits the same violation, the fine applicable to the individual shall be one-half of the fine applicable to an organization.

2. The sanctioning competence of the titles prescribed in Chapter III of this Decree shall be the competence applicable to a single administrative violation committed by an organization. In the case of a fine, the sanctioning competence applicable to an individual shall be one-half of that applicable to an organization.

3. The maximum fine in the field of cybersecurity shall be VND 200.000.000 for an organization and VND 100.000.000 for an individual.

4. Maximum fines in the field of personal data protection:

a) The maximum fine for the administrative violation of purchasing or selling personal data shall be 10 times the proceeds obtained from the violation. Where no proceeds are obtained from the violation, or where the fine calculated based on the proceeds obtained from the violation is lower

than the maximum fine prescribed in Point c of this Clause, the fine prescribed in Point c of this Clause shall apply;

b) The maximum fine imposed on an organization for violating regulations on the cross-border transfer of personal data shall be 5% of the organization's revenue in the immediately preceding year. Where the organization had no revenue in the immediately preceding year, or where the fine calculated based on revenue is lower than the maximum fine prescribed in Point c of this Clause, the fine prescribed in Point c of this Clause shall apply;

c) The maximum fine for other administrative violations in the field of personal data protection shall be VND 3 billion;

d) The maximum fines prescribed in Points a, b, and c of this Clause shall apply to organizations. Where an individual commits the same violation, the maximum fine shall be one-half of the maximum fine applicable to an organization.

Article 8. Penalties for administrative violations in electronic environment

1. Evidence proving violations in the electronic environment:

a) Evidence proving an administrative violation in the electronic environment includes forms of representation of data messages, information, images, audio, digital documents, and other forms of data collected directly or online from electronic devices or information systems of the violating organization or individual, or collected from electronic devices or information systems of other organizations or individuals;

b) Persons competent to impose penalties for administrative violations shall inspect and assess the reliability and integrity of electronic evidence, and may require relevant organizations and individuals to provide data, information, images, audio, digital documents, and other forms of data proving the violation in accordance with the law;

c) Electronic evidence collected in accordance with Point a Clause 1 of this Article shall have legal validity and constitute a basis for handling the administrative violations prescribed in this Decree.

2. Making administrative violation records in the electronic environment:

a) An electronic administrative violation record is a record made, digitally signed, sent, received, retained, and managed by electronic means;

b) The making of an administrative violation record in the electronic environment shall ensure the authentication of the identity of the record maker, the violator, the representative of the violating organization, witnesses, if any, and interpreters, if any. The information and data contained in the record shall not be altered after being digitally signed using legally valid digital signatures by the record maker, the violator, the representative of the violating organization,

witnesses, if any, and interpreters, if any. The integrity, safety, and confidentiality of data shall be ensured in accordance with the law on electronic transactions and the law on cybersecurity;

c) An administrative violation record shall be digitally signed by the person competent to make the record and the violator or lawful representative of the violating organization. Where the violator or representative of the violating organization is unable to use a digital signature in electronic penalty procedures, a biometric authentication method using a facial image or fingerprint shall be used to establish their identity in accordance with the law and in place of the digital signature of the violator or representative of the violating organization;

d) An administrative violation record made in the electronic environment shall have the same legal validity as a record made in paper form and shall constitute a basis for issuing a decision on penalties for administrative violations.

3. Issuance of decisions on penalties for administrative violations in the electronic environment:

a) An electronic decision on penalties for administrative violations is a decision made, digitally signed, sent, retained, and managed by electronic means;

b) A decision on penalties for administrative violations issued in the electronic environment shall bear the legally valid digital signature of the person competent to impose penalties. All contents and data of the decision shall be securely and confidentially retained and shall not be edited or altered after its issuance. Where the violating individual or organization is unable to access the electronic system, the authority competent to impose penalties shall ensure that notification of the penalty decision is provided by text message and email and shall concurrently retain an electronic copy of the decision in the information system used to issue penalty decisions;

c) A decision on penalties for administrative violations issued in the electronic environment shall have the same legal validity as a decision issued in paper form and shall constitute a basis for organizing the enforcement of the penalty decision, collecting and paying fines, and implementing remedial measures in accordance with regulations.

4. The conditions for handling administrative violations in the electronic environment shall comply with Decree No. 118/2021/ND-CP dated December 23, 2021 of the Government of Vietnam, amended by Decree No. 68/2025/ND-CP and Decree No. 190/2025/ND-CP.

Chapter II

ADMINISTRATIVE VIOLATIONS, PENALTIES, AND REMEDIAL MEASURES

Section 1. VIOLATIONS OF REGULATIONS ON PROTECTION OF NATIONAL SECURITY AND MAINTENANCE OF SOCIAL ORDER AND SAFETY IN CYBERSPACE

Article 9. Provision and sharing of information in cyberspace containing unlawful content affecting security and order

1. A fine ranging from VND 5.000.000 to VND 10.000.000 shall be imposed for any of the following violations:

- a) Providing or sharing information for the purpose of promoting, advocating, or enticing others to commit acts infringing upon social security or order;
- b) Providing or sharing information of a threatening nature, inciting conflict or division, or adversely affecting the security and order situation;
- c) Providing or sharing information containing content that incites or induces mass gatherings, thereby affecting social order and safety or the operations of agencies and organizations;
- d) Providing or sharing unverified information relating to history or revolutionary traditions.

2. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations that are not serious enough for criminal prosecution:

- a) Providing or sharing false information concerning national sovereignty, security, or national defense, thereby affecting security and order;
- b) Providing or sharing inappropriate information that adversely affects the sanctity of the nation, national flag, national emblem, national anthem, great persons, leaders, eminent persons, or national heroes;
- c) Providing or sharing inappropriate information relating to ethnicity, belief, religion, gender, or race, thereby causing adverse effects in society;
- d) Creating, posting, or sharing fabricated information in cyberspace, thereby affecting security and order;
- dd) Providing or sharing false or distorted information that affects the normal operations or reputation of agencies, organizations, or the People's administration.

3. Remedial measures:

- a) Mandatory removal or deletion of the violating information in respect of the violations prescribed in Clauses 1 and 2 of this Article;
- b) Mandatory correction of false information in respect of the violations prescribed in Clauses 1 and 2 of this Article.

Article 10. Production and dissemination of information in cyberspace containing content that infringes upon economic management order

1. A fine ranging from VND 5.000.000 to VND 10.000.000 shall be imposed for any of the following violations:

a) Providing or sharing information concerning products, goods, or security instruments that fails to meet the accuracy requirements prescribed by law, thereby affecting the lawful rights and interests of organizations or individuals or affecting market order;

b) Providing or sharing content promoting products, services, equipment, or goods that have not been certified or permitted by a competent authority for use in medical examination and treatment activities in accordance with the law.

2. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

a) Posting or disseminating information concerning the unlawful purchase, sale, exchange, donation, collection, lease, lending, or use of digital accounts, where the violation is not serious enough for criminal prosecution;

b) Posting or disseminating information concerning the purchase or sale of goods or services prohibited by law, where the violation is not serious enough for criminal prosecution;

c) Posting or disseminating information advertising or concerning the purchase, sale, exchange, or donation of counterfeit money, counterfeit security instruments, or counterfeit payment instruments, where the violation is not serious enough for criminal prosecution.

3. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for establishing websites, social networks, accounts, specialized pages, associations or groups on social networks, or electronic forums for posting or disseminating information concerning, or providing instructions on the commission of, the violations prescribed in Clauses 1 and 2 of this Article.

4. Additional penalty: Suspension of operations for a definite period of between 1 and 3 months in respect of an organization committing the violation prescribed in Clause 3 of this Article.

5. Remedial measures:

a) Mandatory removal or deletion of information in cyberspace containing content that infringes upon economic management order, in respect of the violations prescribed in Clauses 1, 2, and 3 of this Article;

b) Mandatory revocation or return of the domain name used for committing the violation prescribed in Clause 3 of this Article;

c) Mandatory correction of information in cyberspace containing content that infringes upon economic management order, in respect of the violations prescribed in Clauses 1, 2, and 3 of this Article;

d) Mandatory remittance of an amount equal to the value of exhibits or means of administrative violations that have been sold, dispersed, or unlawfully destroyed, in respect of the violations prescribed in Clauses 1, 2, and 3 of this Article.

Article 11. Production and dissemination of false or unverified information in cyberspace causing public anxiety and affecting social order

1. A fine ranging from VND 5.000.000 to VND 10.000.000 shall be imposed for any of the following violations:

- a) Providing or sharing information containing content that is inconsistent with fine traditions and customs or social ethics, or that is likely to adversely affect the community;
- b) Providing or sharing information containing content that encourages or provides instructions on committing acts contrary to the law, where the violation is not serious enough for criminal prosecution;
- c) Providing or sharing information concerning medical examination or treatment methods, therapies, remedies, or techniques that have not been permitted by a competent authority or certified in accordance with specialized regulations;
- d) Providing or sharing information recommending the modification, postponement, or non-application of medical examination or treatment methods or protocols recognized by a competent authority without an appropriate professional recommendation.

2. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

- a) Producing or disseminating false or unverified information that affects the lawful rights and interests of organizations or individuals or the information environment in cyberspace;
- b) Producing or disseminating information containing content that is inconsistent with fine traditions and customs or social ethics, or that is likely to adversely affect the community;
- c) Producing or disseminating information containing content that encourages or provides instructions on committing acts contrary to the law, where the violation is not serious enough for criminal prosecution;
- d) Producing or disseminating information concerning medical examination or treatment methods, therapies, remedies, or techniques that have not been permitted by a competent authority or certified in accordance with specialized regulations;
- dd) Producing or disseminating information recommending the modification, postponement, or non-application of medical examination or treatment methods or protocols recognized by a competent authority without an appropriate professional recommendation.

3. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for establishing or administering websites, social networks, accounts, associations, groups, or specialized pages on social networks, or electronic forums for posting information concerning, or providing instructions on the commission of, the violations prescribed in Clauses 1 and 2 of this Article.

4. The penalties prescribed in Points d and dd Clause 1 and in Clause 2 of this Article shall not apply where an individual shares personal experience relating to medical examination or treatment without the purpose of advertising, providing professional advice, providing instructions as a substitute for treatment, or obtaining profits from the provision of medical examination or treatment products, services, or methods.

5. Additional penalties:

a) Confiscation of exhibits and means used for committing the violations prescribed in Clauses 1, 2, and 3 of this Article;

b) Suspension of operations for a definite period of between 1 and 3 months in respect of an enterprise committing the violation prescribed in Clause 3 of this Article.

6. Remedial measures:

a) Mandatory removal or deletion of fabricated or false information in cyberspace that causes public anxiety and affects social order, in respect of the violations prescribed in Clauses 1, 2, and 3 of this Article;

b) Mandatory revocation or return of the domain name used for committing the violation prescribed in Clause 3 of this Article;

c) Mandatory correction of fabricated or false information in cyberspace intended to cause public anxiety and affect social order, in respect of the violations prescribed in Clauses 1, 2, and 3 of this Article;

d) Mandatory return or remittance of illegal profits obtained from the violations prescribed in Clauses 1, 2, and 3 of this Article.

Article 12. Violations of regulations on responsibilities for preventing and handling information in cyberspace containing unlawful content

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

a) Managing, operating, or having the ability to control websites, social networks, accounts, associations, groups, or specialized pages on social networks without implementing measures to prevent, detect, block, remove, or delete information containing unlawful content;

b) Failing to implement managerial and technical measures to prevent, detect, block, remove, or delete information containing unlawful content.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Managing, operating, or having the ability to control websites, social networks, accounts, associations, groups, or specialized pages on social networks without implementing measures to prevent, detect, block, remove, or delete information containing unlawful content at the request of a competent functional authority;

b) Failing to provide information or documents concerning violations of the law posted or shared on information systems, products, or services of organizations or individuals at the request of a competent functional authority.

3. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to provide a connection gateway or the technical conditions necessary for information security and cybersecurity assurance duties at the request of the Ministry of Public Security of Vietnam;

b) Failing to block or cease the provision of telecommunications or Internet services in cases involving riots or violent disturbances, or the use of telecommunications services to infringe upon national security or oppose the State of the Socialist Republic of Vietnam;

c) Failing to implement or maintain technical measures at the request of a competent state authority to block access to unlawful websites, applications, platforms, or domain names, thereby allowing users in Vietnam to continue accessing or using services, platforms, or domain names subject to blocking;

d) Failing to invest in, update, or upgrade technical systems and network technologies to meet state management requirements concerning cybersecurity and data security; or failing to proactively review and update technological solutions and technical plans to ensure effective blocking and minimize access to unlawful websites, applications, platforms, or domain names at the request of a competent state authority;

dd) Failing to comply with a decision to mobilize part or all of the Internet infrastructure for the purpose of handling a dangerous cybersecurity situation;

e) Failing to provide information for the protection of national security at the request of the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam.

4. Additional penalty: Suspension of operations for a definite period of between 1 and 3 months in respect of an enterprise committing any of the violations prescribed in Clauses 2 and 3 of this Article.

5. Remedial measures:

a) Mandatory removal or deletion of information in cyberspace containing unlawful content, in respect of the violations prescribed in Clauses 1, 2, and 3 of this Article;

b) Mandatory revocation or return of the domain name used for committing the violation prescribed in Point b Clause 2 of this Article.

Article 13. Violations of regulations on protection of information constituting personal secrets, work secrets, business secrets, family secrets, and private life in cyberspace

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

a) Posting in cyberspace information constituting work secrets, business secrets, personal secrets, family secrets, or private life, thereby affecting the honor, reputation, dignity, or lawful rights and interests of agencies, organizations, or individuals, where the violation is not serious enough for criminal prosecution;

b) Failing to comply with a request from a specialized cybersecurity protection force concerning the prevention and combating of cyber espionage or the protection of information constituting state secrets in accordance with the law;

c) Unlawfully altering, destroying, or disabling technical measures developed and used to protect information constituting state secrets.

2. Additional penalties:

a) Confiscation of exhibits and means used for committing the administrative violation prescribed in Points a and c Clause 1 of this Article;

b) Suspension of operations for a definite period of between 1 and 3 months in respect of the violations prescribed in Points b and c Clause 1 of this Article.

3. Remedial measures:

a) Mandatory development and implementation of measures for protecting state secrets and preventing the disclosure or loss of state secrets through technical channels, in respect of the violations prescribed in Clause 1 of this Article;

b) Mandatory destruction of products, equipment, services, or software that cause the disclosure or loss of state secrets or fail to ensure cybersecurity, in respect of the violations prescribed in Points a and c Clause 1 of this Article. Where documents or objects containing state secrets are involved, the Law on Protection of State Secrets shall apply;

c) Mandatory re-inspection of the cybersecurity of products, equipment, services, and software used for protecting state secrets, in respect of the violation prescribed in Point a Clause 1 of this Article;

d) Mandatory remittance of an amount equal to the value of exhibits or means of administrative violations that have been sold, dispersed, or unlawfully destroyed, in respect of the violation prescribed in Point a Clause 1 of this Article.

Article 14. Violations of regulations on prevention and combating of acts involving use of cyberspace, information technology, or electronic means to infringe upon economic management order, where such violations are not serious enough for criminal prosecution

1. A fine ranging from VND 5.000.000 to VND 10.000.000 shall be imposed for selling, leasing, lending, or donating information concerning one's own digital accounts, including bank accounts, bank cards, electronic wallet accounts, mobile money accounts, securities accounts, transaction accounts, insurance accounts, tax accounts, and other digital accounts with financial transaction functions.

2. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

- a) Using a false identity, forged documents or dossiers, or unlawfully using another person's information to establish an enterprise or establish or register a bank account, bank card, electronic wallet account, mobile money account, securities account, transaction account, insurance account, tax account, or another digital account with financial transaction functions, where the violation is not serious enough for criminal prosecution;
- b) Using a digital account with financial transaction functions as an intermediary instrument to conduct transactions or receive, transfer, or make payments to another beneficiary, except where licensed by a competent authority;
- c) Renting, leasing out, providing, or using a service for receiving text messages, calls, or other forms of communication to authenticate information or identify a digital account with financial transaction functions, except where licensed by a competent authority;
- d) Using a digital account to unlawfully purchase, sell, trade, or exchange foreign currencies.

3. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Establishing or using a website, digital account, or electronic interface that causes confusion as to the identity of the agency, organization, or individual providing the information;
- b) Providing, sharing, or using digital content in cyberspace that fails to comply with regulations on copyrights, related rights, or intellectual property, where the violation is not serious enough for criminal prosecution;
- c) Using authentication credentials, login information, or access rights for a digital account contrary to the law;

d) Establishing, operating, or providing services for, or supporting the operations of, an exchange, application, or digital platform that fails to satisfy the conditions for service provision prescribed by law;

dd) Providing information, advertising, or conducting business involving goods that fail to comply with the laws on commerce, quality, origin, provenance, or conditions for circulation, where the violation is not serious enough for criminal prosecution.

4. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Providing, establishing, or operating an information system, website, application, or exchange for peer-to-peer lending, virtual currencies, virtual assets, or other similar forms without a license or approval from a competent authority;

b) Providing, establishing, or operating an information system, website, application, or exchange for foreign currencies, metals, oil, gemstones, or other similar forms without a license or approval from a competent authority;

c) Providing, sending, or disseminating text messages, calls, or emails using the name or identifying information of an agency or organization contrary to the law.

5. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Using cyberspace to interfere with, alter, or falsify transaction information or recipient account information contrary to the law;

b) Using cyberspace to raise capital or receive or distribute funds in a manner that fails to ensure transparency or comply with the law;

c) Organizing or conducting multi-level marketing activities in cyberspace without satisfying the operating conditions prescribed by law;

d) Providing or sharing information concerning, or conducting, securities transactions in cyberspace contrary to the law;

dd) Using cyberspace to solicit, receive, manage, or distribute contributions or community support without ensuring publicity and transparency as prescribed by law;

e) Using information concerning a digital account, social networking account, or electronic account of an organization or individual without proper authority or the account holder's consent.

6. A fine ranging from VND 70.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

a) Opening a digital account contrary to the procedures prescribed by law, or maintaining a digital account with financial transaction functions using fabricated identity information or information that does not exist in the National Population Database or the database of organizations and enterprises, including bank accounts, bank cards, electronic wallet accounts, mobile money accounts, securities accounts, transaction accounts, and other digital accounts with financial transaction functions;

b) Opening a digital account for a person included on the list of persons prohibited from opening and using digital accounts.

7. Additional penalty: Confiscation of exhibits, means, and money held in digital accounts in respect of any of the violations prescribed in Clause 1 of this Article.

8. Remedial measures:

a) Mandatory removal or deletion of information in respect of the violations prescribed in Points b and dd Clause 3 of this Article;

b) Mandatory remittance of an amount equal to the value of exhibits or means of administrative violations that have been sold, dispersed, or unlawfully destroyed, in respect of the violations prescribed in Clauses 1, 2, 3, 4, 5, and 6 of this Article.

Article 15. Violations of regulations on prevention and combating of acts involving use of cyberspace, information technology, or electronic means to infringe upon social order, where such violations are not serious enough for criminal prosecution

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

a) Posting or sharing information promoting prize-redeemable games in cyberspace contrary to the law, where the violation is not serious enough for criminal prosecution;

b) Using the information or identifying elements of an agency or organization when contacting or exchanging information in cyberspace without ensuring authenticity as prescribed by law;

c) Posting or sharing information concerning belief or spiritual activities on social networking platforms or messaging applications contrary to law;

d) Posting or sharing information in cyberspace that advocates or encourages unlawful racing, where the violation is not serious enough for criminal prosecution;

dd) Posting or promoting information concerning wild animals in cyberspace contrary to the law on wildlife protection;

- e) Posting images, videos, audio, or written content of a pornographic or depraved nature on social networking platforms, messaging applications, or websites, where the violation is not serious enough for criminal prosecution;
- g) Live-streaming content, images, or conduct in cyberspace that is inconsistent with cultural standards or social ethics;
- h) Establishing a website or digital platform for posting information concerning the provision of services contrary to the law;
- i) Posting or sharing cinematographic works, television programs, videos, music, or other digital content without satisfying regulations on copyrights and related rights;
- k) Live-streaming or sharing content from sporting events, artistic performances, or cinematographic works originating from sources that have not been authorized for dissemination in accordance with regulations;
- l) Reproducing, providing, or distributing software or mobile applications without satisfying the conditions for use prescribed by the law on intellectual property rights;
- m) Using artificial intelligence (AI) technology to create digital products containing similar content or utilizing original works without satisfying the requirements concerning intellectual property rights prescribed by law;
- n) Producing, providing, or sharing software or tools that facilitate interference with or alteration of copyright management mechanisms for software or operating systems contrary to the law;
- o) Providing devices or software that facilitate the reception or decoding of television signals without satisfying the conditions prescribed by law;
- p) Providing instructions or sharing methods for accessing websites, applications, or digital platforms whose scope of access has been restricted in accordance with the law.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Establishing or operating a website, social network, information system, or application that provides games or prize-redeemable programs in cyberspace without satisfying the conditions prescribed by law;
- b) Providing information technology services, hardware, software, domain names, applications, or digital platforms containing content that fails to comply with regulations on copyrights, related rights, or industrial property rights, where the violation is not serious enough for criminal prosecution;

c) Establishing websites, social networks, specialized pages on social networks, information systems, or applications containing advertisements for prostitution or pornographic or depraved content, where the violation is not serious enough for criminal prosecution;

d) Organizing the filming or live-streaming of pornographic or depraved images on information systems, websites, or social networks, where the violation is not serious enough for criminal prosecution;

dd) Providing information technology services, hardware, software, or other services that support or facilitate the filming or live-streaming of pornographic or depraved content, where the violation is not serious enough for criminal prosecution;

e) Failing to moderate, block, or remove pornographic or depraved content, content relating to social evils, or other violations of the law from information systems, websites, or social networks, where the violation is not serious enough for criminal prosecution;

g) Posting or sharing information in cyberspace concerning goods, substances, or products included on a list of those prohibited from business or circulation by law, where the violation is not serious enough for criminal prosecution;

h) Posting or sharing information in cyberspace concerning the purchase or sale of human tissues or body parts contrary to the law, where the violation is not serious enough for criminal prosecution;

i) Posting or sharing information that provides instructions on or encourages the commission of acts contrary to the law;

k) Posting information in cyberspace promoting lending services that fail to comply with the law on interest rates and lending activities;

l) Posting information in cyberspace concerning the purchase or sale of weapons, explosives, combat gear, uniforms, rank insignia, badges, or identification numbers of the People's Public Security Force or the Vietnam People's Army;

m) Providing online payment services to applications or websites containing pornographic or depraved content or engaging in prostitution-related activities, where the violation is not serious enough for criminal prosecution.

3. Additional penalty: Confiscation of exhibits and means used for committing the violations prescribed in Clauses 1 and 2 of this Article.

4. Remedial measures:

a) Mandatory removal or deletion of information in respect of the violations prescribed in Clause 1 of this Article;

- b) Mandatory recall or destruction of products or equipment, or cessation of the provision of services, that are harmful to cybersecurity; fail to satisfy the conditions, standards, or technical regulations prescribed by law; are provided without a license; or are provided contrary to the relevant license, in respect of the violations prescribed in Clause 2 of this Article;
- c) Mandatory removal of cybersecurity-harmful features or components from programs, products, equipment, services, or software, in respect of the violations prescribed in Clause 2 of this Article;
- d) Mandatory return or remittance of illegal profits obtained from the violations prescribed in Clauses 1 and 2 of this Article;
- dd) Mandatory remittance of an amount equal to the value of exhibits or means of administrative violations that have been sold, dispersed, or unlawfully destroyed, in respect of the violations prescribed in Clauses 1 and 2 of this Article.

Section 2. VIOLATIONS OF REGULATIONS ON PREVENTION AND COMBATING OF CYBERATTACKS

Article 16. Violations of regulations on prevention and combating of cyberattacks

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Providing, sharing, or using computer programs that affect the safety or operational stability of information systems, computer networks, or electronic means;
- b) Introducing programs, code, or applications into an information system, thereby affecting the management, retention, or utilization of data of organizations or individuals;
- c) Interfering with or otherwise affecting the operational stability or data transmission capacity of telecommunications networks, the Internet, computer networks, or electronic means contrary to the law;
- d) Accessing, affecting, or interfering with data retained or transmitted through telecommunications networks, the Internet, computer networks, or electronic means without proper authority or contrary to law, where the violation is not serious enough for criminal prosecution;
- dd) Utilizing, using, providing, or sharing information or data, or discovering, testing, or using weaknesses or technical vulnerabilities of an information system, contrary to regulations on network safety and cybersecurity;
- e) Committing an act that affects the normal operation of telecommunications networks, the Internet, computer networks, or electronic means;

g) Failing to fully and promptly provide information or documents relating to a cyberattack at the request of a competent authority in accordance with the law.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Producing, purchasing, selling, exchanging, or donating computer programs or information technology software that is harmful to computer networks, telecommunications networks, or electronic means, where the violation is not serious enough for criminal prosecution;

b) Failing to cooperate with a specialized cybersecurity protection force in implementing measures to prevent and eliminate a cyberattack;

c) Providing unlawful cyberattack services, where the violation is not serious enough for criminal prosecution.

3. Additional penalties:

a) Confiscation of exhibits and means used for committing the violations prescribed in Clauses 1 and 2 of this Article;

b) Expulsion from the territory of the Socialist Republic of Vietnam of a foreigner committing any of the violations prescribed in Clauses 1 and 2 of this Article.

4. Remedial measures:

a) Mandatory recall of products or equipment or cessation of the provision of services that are harmful to cybersecurity, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

b) Mandatory destruction or irreversible deletion of data that has been unlawfully appropriated, purchased, sold or exchanged, in respect of the violations prescribed at Points a and b Clause 1 and Point a Clause 2 of this Article;

c) Mandatory return of IP addresses, autonomous system numbers (ASNs), domain names, and digital accounts, in respect of the violations prescribed in Points a, b, c, d, dd, and e Clause 1 and Points a and c Clause 2 of this Article;

d) Mandatory recovery of illegal profits obtained from the violations prescribed in Point dd Clause 1 and Point a Clause 2 of this Article;

dd) Mandatory remittance of an amount equal to the value of exhibits or means of administrative violations that have been sold, dispersed, or unlawfully destroyed, in respect of the violations prescribed in Clauses 1 and 2 of this Article.

Article 17. Violations of regulations on prevention and combating of cyberterrorism

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

- a) Sharing, commenting on, or disseminating information containing content that supports or promotes activities violating the law on terrorism in cyberspace, where the violation is not serious enough for criminal prosecution;
- b) Providing or sharing information containing content that calls for, advocates, or provides instructions on committing acts violating the law on network safety or cybersecurity, where the violation is not serious enough for criminal prosecution;
- c) Posting or sharing information containing content that advocates violence or extremism or adversely affects security, order, or social safety, where the violation is not serious enough for criminal prosecution.

2. A fine ranging from VND 20.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Assisting or facilitating the use of cyberspace to provide, receive, or solicit financial support contrary to the law on prevention and combating of terrorism, where the violation is not serious enough for criminal prosecution;
- b) Assisting organizations or individuals in using cyberspace to circumvent, evade, or reduce the effectiveness of network safety or cybersecurity safeguards implemented by a competent authority, where the violation is not serious enough for criminal prosecution;
- c) Calling for or advocating the mobilization of financial resources in cyberspace contrary to the law on prevention and combating of terrorism, where the violation is not serious enough for criminal prosecution;
- d) Providing or sharing inaccurate information relating to terrorist activities or terrorism financing, or committing an act that affects the counterterrorism activities of a competent authority, where the violation is not serious enough for criminal prosecution.

3. Additional penalties:

- a) Confiscation of exhibits and means used for committing the violations prescribed in Clauses 1 and 2 of this Article;
- b) Expulsion from the territory of the Socialist Republic of Vietnam of a foreigner committing any of the violations prescribed in Clauses 1 and 2 of this Article.

4. Remedial measures:

a) Mandatory removal or deletion of programs or software, recall or destruction of products or equipment, or cessation of the provision of services that are harmful to cybersecurity, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

b) Mandatory removal from the territory of the Socialist Republic of Vietnam or re-export of goods, articles, or means, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

c) Mandatory destruction or irreversible deletion of data that has been unlawfully appropriated, purchased, sold, or exchanged, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

d) Mandatory deletion and correction of false or misleading information, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

dd) Mandatory recall of products, equipment, services, or software that fail to satisfy quality requirements, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

e) Mandatory revocation of subscriber numbers, prefixes, and telecommunications numbering resources; Internet resources, domain names, Internet Protocol addresses (IP addresses) and autonomous system numbers (ASNs); and management codes and service provision numbers, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

g) Mandatory return of IP addresses, ASNs, domain names, and digital accounts, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

h) Mandatory recovery of illegal profits obtained from the violations prescribed in Clauses 1 and 2 of this Article.

Article 18. Violations of regulations on prevention and handling of dangerous cybersecurity situations

1. A fine ranging from VND 25.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to cooperate in blocking, removing, or deleting inflammatory information in cyberspace that poses a risk of riots, security disturbances, or terrorism within 24 hours from the time a request is made by the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam;

b) Failing to cooperate, or delaying cooperation for more than 24 hours after receiving a request from the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam, in implementing technical and professional solutions to prevent, detect, or handle a dangerous cybersecurity situation;

c) Failing to cooperate, or delaying cooperation for more than 24 hours after receiving a request from the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam, with the specialized cybersecurity protection force in preventing, detecting, or handling a dangerous cybersecurity situation;

d) Failing to cooperate, or delaying cooperation for more than 24 hours after receiving a request from the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam, in implementing cybersecurity prevention and emergency response plans or preventing, eliminating, or mitigating damage caused by a dangerous cybersecurity situation;

dd) Failing to cooperate, or delaying cooperation for more than 24 hours after receiving a request from the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam, in collecting relevant information or continuously monitoring and supervising a dangerous cybersecurity situation;

e) Failing to cooperate, or delaying cooperation for more than 24 hours after receiving a request from the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam, in suspending the provision of network information within a specific area or disconnecting an international network gateway in response to a dangerous cybersecurity situation;

g) Failing to deploy personnel and means to prevent or eliminate a dangerous cybersecurity situation.

2. Remedial measure: Mandatory implementation of necessary technical and managerial measures to prevent and remedy risks to network safety or cybersecurity caused by any of the violations prescribed in Clause 1 of this Article.

Section 3. VIOLATIONS OF REGULATIONS ON IMPLEMENTATION OF CYBERSECURITY PROTECTION ACTIVITIES

Article 19. Violations of regulations on unlawful provision or use of online information

1. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Gaining unauthorized access to another person's network or digital device to take control of the digital device; alter or delete information stored on the digital device; modify the configuration parameters of the digital device; or collect another person's information, where the violation is not serious enough for criminal prosecution;

b) Infiltrating, modifying, or deleting information belonging to another organization or individual in the network environment;

c) Obstructing the provision of services by an information system;

d) Preventing access to information belonging to another organization or individual in the network environment, except where permitted by law;

dd) Compromising the security or confidentiality of information belonging to another organization or individual that is exchanged, transmitted, or retained in the network environment.

2. Additional penalty: Expulsion from the territory of the Socialist Republic of Vietnam of a foreigner committing any of the violations prescribed in Clause 1 of this Article.

Article 20. Violations of regulations on management of transmission of information over networks

1. A fine ranging from VND 25.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Sending commercial information to the electronic address of a recipient without the recipient's prior consent or after the recipient has refused to receive such information;

b) Failing to provide a method through which the recipient may refuse to receive information.

2. A fine ranging from VND 25.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Falsifying the origin of information transmitted over a network;

b) Failing to provide the necessary technical and professional conditions at the request of a competent state authority.

3. A fine ranging from VND 50.000.000 to VND 75.000.000 shall be imposed for failing to implement blocking measures or take action after receiving a notification from an organization or individual concerning the transmission of information in violation of the law.

4. Remedial measure: Mandatory removal of unlawful information sent or disseminated over a network, in respect of the violation prescribed in Point a Clause 1 of this Article.

Article 21. Violations of regulations on cybersecurity incident response

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

a) Failing to publish information concerning the address for receiving incident reports on a website or web portal;

b) Failing to declare dossiers or provide or update information concerning incident response contact points, cybersecurity technical personnel, or incident response activities under its

management to the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam;

c) Failing to update information concerning an incident response contact point within the prescribed time limit following a change;

d) Violating the operating regulations of the national cybersecurity incident response network or failing to comply with the coordination requirements of the coordinating authority.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Failing to report to the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam upon receiving information concerning or detecting an incident involving an information system under its management;

b) Failing to conduct incident response activities and submit reports in accordance with regulations after detecting an incident or receiving a request from the specialized cybersecurity protection force.

3. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing, upon request, to consolidate information and report developments concerning an incident to the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam;

b) Failing to establish or designate a specialized cybersecurity incident response unit, or failing to establish an incident response team;

c) Failing to record or receive an incident notification, or failing to report a cybersecurity incident in accordance with the prescribed process;

d) Failing to develop a cybersecurity incident response plan;

dd) Failing to fully comply with the Ministry of Public Security of Vietnam's incident response coordination requirements.

4. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Failing to appoint a contact point to cooperate in incident response activities or failing to participate in the national cybersecurity incident response network;

b) Failing to comply with the incident response coordination requirements of the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam;

- c) Failing to provide premises, connection gateways, and the necessary technical conditions at the request of the Ministry of Public Security of Vietnam;
- d) Failing to organize incident response activities within the sector, geographical area, or scope under its management;
- dd) Failing to cooperate with the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam, service providers, and functional authorities in restoring essential operations, data, or connections to minimize damage to information systems or adverse effects on society;
- e) Failing to cooperate during the period in which an incident has not yet been completely remedied;
- g) Failing to address the consequences of an incident involving its information system that affects the public or other agencies or organizations;
- h) Failing to retain or provide information relating to subscriber IP addresses, servers, Internet of Things (IoT) devices, log files, or Domain Name System (DNS) service logs under its management;
- i) Failing to establish an environment for installing monitoring and sampling equipment and providing network data feeds;
- k) Failing to establish a permanent 24/7 contact point or provide personnel and material resources ready to cooperate and implement solutions for responding to and remedying the consequences of an incident where the source of the attack is determined to originate from a subscriber of the enterprise or where requested by the Ministry of Public Security of Vietnam.

5. Remedial measures:

- a) Mandatory restoration of the information system to its original state, in respect of the violations prescribed in Clauses 1, 2, 3, and 4 of this Article;
- b) Mandatory recovery or removal of data, information, or network connections that compromise cybersecurity, in respect of the violations prescribed in Clauses 1, 2, 3, and 4 of this Article.

Article 22. Violations of regulations on prevention, detection, blocking, and handling of malware

1. A fine ranging from VND 15.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Failing to implement managerial measures or measures to prevent, detect, or block the dissemination of malware;

b) Failing to report to a competent state authority on the malware filtering system used during the transmission, receipt, or retention of information on its system in accordance with the law.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to maintain a malware filtering system during the transmission, receipt, or retention of information on the systems of an enterprise providing email, information transmission, or information retention services;

b) Failing to prevent, block, or handle the dissemination of malware in accordance with the instructions or requirements of a competent state authority;

c) Failing to implement a technical and professional system for the timely prevention, detection, blocking, and handling of malware.

3. Additional penalty: Deprivation of the right to use the license to provide social networking services for a definite period of between 1 and 3 months in respect of a repeated commission of any of the violations prescribed in Clauses 1 and 2 of this Article.

4. Remedial measures:

a) Mandatory restoration of an information system affected by malware to its original state, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

b) Mandatory implementation of measures to remedy the cybersecurity compromise, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

c) Mandatory removal or destruction of malware, malicious code, or malicious data unlawfully disseminated, in respect of the violations prescribed in Clauses 1 and 2 of this Article.

Article 23. Violations of regulations on security monitoring and information system protection measures

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Failing to promulgate regulations on cybersecurity assurance in the design, construction, management, operation, use, upgrading, or decommissioning of an information system;

b) Failing to prepare a dossier proposing the information system security level for an information system classified from Level 3 to Level 5;

c) Putting an information system classified from Level 3 to Level 5 into operation before its cybersecurity level has been approved;

d) Failing to fully implement cybersecurity assurance measures in accordance with the approved cybersecurity dossier for an information system classified from Level 3 to Level 5.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to inspect or monitor compliance with cybersecurity assurance regulations or retain system logs as prescribed, or failing to assess the effectiveness of the managerial and technical measures implemented;

b) Failing to cooperate with the information system administrator in monitoring information system security at the request of a competent state authority;

c) Failing to organize, urge, inspect, or supervise cybersecurity assurance activities;

d) Obstructing or failing to exchange system monitoring information or data between a unit hired by the information system administrator and the specialized cybersecurity protection force.

3. Additional penalty: Deprivation of the right to use the license to establish a news aggregator site for a definite period of between 1 and 6 months in respect of a repeated commission of any of the violations prescribed in Clauses 1 and 2 of this Article.

4. Remedial measures:

a) Mandatory restoration of the information system to its original state, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

b) Mandatory implementation of measures to remedy a cybersecurity compromise or risk of a cybersecurity compromise, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

c) Mandatory removal of cybersecurity-related violating elements from the design, construction, management, operation, use, upgrading, or decommissioning of the information system, in respect of the violations prescribed in Clauses 1 and 2 of this Article.

Article 24. Violations of regulations on information system security assurance by security level

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for failing to prepare a dossier proposing an information system security level or failing to organize the appraisal or approval of such dossier in accordance with regulations.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for failing to expand or upgrade a nationally important information system before putting it into operation or utilization.

3. Additional penalty: Deprivation of the right to use the license to establish a news aggregator site for a definite period of between 1 and 3 months in respect of a repeated commission of any of the violations prescribed in Clauses 1 and 2 of this Article.

4. Remedial measures:

a) Mandatory restoration of the information system to its original state, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

b) Mandatory implementation of measures to remedy a risk of a cybersecurity compromise or an actual cybersecurity compromise, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

c) Mandatory removal of cybersecurity-related violating elements, in respect of the violations prescribed in Clauses 1 and 2 of this Article.

Article 25. Violations of regulations on prevention of information conflicts in cyberspace

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

a) Failing to provide notification or complete information upon detecting signs or acts causing an information conflict in cyberspace, or upon discovering that information or an information system has been compromised;

b) Failing to receive or process information concerning an information conflict in cyberspace for the purpose of incident response and prevention of the information conflict;

c) Failing to cooperate with specialized agencies in accurately identifying the source of an information conflict in cyberspace;

d) Failing to cooperate with specialized agencies in eliminating an information conflict in cyberspace.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Failing to block or filter information at the request of specialized agencies or upon a reasonable request from a party affected by an information conflict in cyberspace;

b) Failing to block destructive information originating from its own information system, or failing to cooperate in identifying the source of, repelling, or remedying the consequences of a cyberattack originating from the information system of a domestic or foreign organization or individual;

c) Failing to develop a plan to remedy an information conflict in cyberspace falling within its management;

d) Failing to consolidate information and report the results of remedying an information conflict in cyberspace to a specialized agency;

dd) Failing to cooperate in remedying an information conflict in cyberspace.

3. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for failing to remedy an information conflict in cyberspace falling within its management.

4. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for failing to cooperate in identifying the source of, or remedying the consequences of, an information conflict in cyberspace.

5. Remedial measures:

a) Mandatory implementation of measures to prevent, block, filter, eliminate, and remedy information conflicts in cyberspace, in respect of the violations prescribed in Clauses 2, 3, and 4 of this Article;

b) Mandatory restoration of the normal operation of the information system, in respect of the violations prescribed in Clauses 1, 2, 3, and 4 of this Article.

Article 26. Violations of regulations on cybersecurity protection for information systems important to national security

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations of regulations on the identification of information systems important to national security:

a) Failing to conduct, or failing to adequately conduct as prescribed, a review to identify information systems important to national security among the information systems under its management;

b) Failing to review and identify information systems important to national security among the information systems under its management after receiving a notification from the specialized cybersecurity protection force;

c) Failing to send, according to the decentralization of management, to the Ministry of Public Security of Vietnam, the Ministry of National Defense of Vietnam, or the Government Cipher Committee the dossiers of nationally important information systems approved by the Prime Minister of Vietnam for the establishment of the list of information systems important to national security;

d) Failing to transfer, according to the decentralization of management, to the Ministry of Public Security of Vietnam, the Ministry of National Defense of Vietnam, or the Government Cipher Committee a cybersecurity-level appraisal dossier considered to provide sufficient grounds for inclusion in the list of information systems important to national security, for appraisal of the dossier proposing the inclusion of the information system in such list.

2. A fine ranging from VND 30.000.000 to VND 40.000.000 shall be imposed for any of the following violations of regulations on cybersecurity appraisal:

a) Failing to conduct a cybersecurity appraisal as a basis for deciding on the construction of an information system that meets the criteria for classification as an information system important to national security;

b) Failing to conduct a cybersecurity appraisal as a basis for upgrading an information system that meets the criteria for classification as an information system important to national security.

3. A fine ranging from VND 40.000.000 to VND 50.000.000 shall be imposed for any of the following violations relating to cybersecurity inspection and monitoring:

a) Failing to assess whether an information system satisfies cybersecurity conditions before putting it into operation or use;

b) Failing to develop cybersecurity assurance regulations, procedures, and plans, or failing to appoint personnel to operate and administer the system;

c) Failing to develop a plan for responding to and remedying cybersecurity incidents involving the information system in accordance with the law;

d) Failing to develop technical measures for cybersecurity monitoring and protection or measures for protecting the system;

dd) Failing to develop measures for protecting state secrets and preventing the disclosure or loss of state secrets through technical channels;

e) Failing to implement physical security measures in accordance with the law;

g) The administrator of an information system important to national security failing to conduct cybersecurity inspection or monitoring of an information system under its management in accordance with the law;

h) Failing to cooperate with the specialized cybersecurity protection force during cybersecurity inspection or monitoring in accordance with the law;

i) Failing to implement or participate in incident response or remediation activities when a cybersecurity incident occurs or at the request of the force responsible for coordinating such activities;

- k) Failing to promptly report to the specialized cybersecurity protection force a serious cybersecurity incident involving an information system under its management;
- l) Failing to implement measures in accordance with the instructions of the specialized cybersecurity protection force and other appropriate measures to prevent, handle, and remedy consequences within 24 hours after receiving a notification.

4. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

- a) Failing to conduct an annual cybersecurity inspection;
- b) Failing to conduct cybersecurity inspection or monitoring when required for the state management of cybersecurity;
- c) Failing to provide written notification of cybersecurity inspection results to the specialized cybersecurity protection force in accordance with regulations;
- d) Failing to remedy weaknesses or security vulnerabilities within the prescribed time limit in accordance with the recommendations of the specialized cybersecurity protection force;
- dd) Violating cybersecurity assurance regulations, procedures, or plans applicable to an information system important to national security;
- e) Violating regulations concerning personnel responsible for system operation and administration or cybersecurity protection;
- g) Violating regulations on cybersecurity assurance conditions applicable to equipment, hardware, or software constituting components of the system;
- h) Violating regulations on technical or physical security measures for cybersecurity monitoring and protection.

5. Remedial measures:

- a) Mandatory implementation of cybersecurity safeguards for information systems important to national security, in respect of the violations prescribed in Clauses 1, 2, 3, and 4 of this Article;
- b) Mandatory correction of cybersecurity appraisal, assessment, inspection, or certification results, in respect of the violations prescribed in Clauses 2, 3, and 4 of this Article.

Article 27. Violations of regulations on cybersecurity protection for information systems not included in list of information systems important to national security

1. A fine ranging from VND 25.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Failing to cooperate with the specialized cybersecurity protection force in implementing cybersecurity protection measures upon discovering that an information system under its management is connected with an act violating the law on cybersecurity;
 - b) Failing to notify the specialized cybersecurity protection force upon discovering a violation of the law on cybersecurity involving an information system of a state authority or a central or local political organization;
 - c) Failing to comply, or failing to fully comply, with a request from the specialized cybersecurity protection force to remedy weaknesses, security vulnerabilities, or violations of the law on cybersecurity.
2. Remedial measure: Mandatory implementation of cybersecurity safeguards in accordance with regulations, in respect of the violations prescribed in Clause 1 of this Article.

Article 28. Violations of regulations on cybersecurity protection for national cyberspace infrastructure and international network gateways

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:
- a) Failing to cooperate with the specialized cybersecurity protection force in conducting cybersecurity monitoring of national cyberspace infrastructure or international network gateways;
 - b) Failing to cooperate or provide information or data for the investigation and handling of violations of the law after receiving a written request;
 - c) Failing to provide premises, connection gateways, conditions, or necessary technical and professional measures for the specialized cybersecurity protection force to perform cybersecurity protection duties in accordance with the law;
 - d) Failing to implement cybersecurity protection measures or comply with the cybersecurity protection requirements of the specialized cybersecurity protection force.
2. Remedial measure: Mandatory implementation of cybersecurity safeguards in accordance with regulations, in respect of the violations prescribed in Clause 1 of this Article.

Article 29. Violations of regulations on network information security assurance

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:
- a) Failing to authenticate information when a user registers a digital account;
 - b) Failing to ensure the confidentiality of users' information or accounts.

2. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

- a) Failing, within 24 hours after receiving a request from the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam, to prevent the sharing of information, or delete information and remove services or applications containing content that violates the Law on Cybersecurity, or failing to retain system logs for the period prescribed by law for the verification, investigation, and handling of violations of the law on cybersecurity; in an emergency threatening national security, failing to block or delete the information within 6 hours;
- b) Providing services on telecommunications networks or the Internet, or value-added services, to organizations or individuals that post in cyberspace information containing the content prescribed in Clauses 1, 2, and 3 of Article 13 or Clauses 1 and 2 of Article 14 of the Law on Cybersecurity; or failing to cease the provision of such services at the request of the specialized cybersecurity protection force or a competent functional authority;
- c) When collecting, utilizing, analyzing, or processing personal information data, data concerning the relationships of service users, or data generated by service users in Vietnam, failing to implement data protection measures prescribed by law or retain such data in Vietnam for the period prescribed by the Government of Vietnam;
- d) A foreign enterprise providing services on telecommunications networks or the Internet, or value-added services in cyberspace in Vietnam, failing to establish a branch or representative office in Vietnam.

3. Remedial measures:

- a) Mandatory implementation of network information security safeguards in accordance with regulations, in respect of the violations prescribed in Clauses 1 and 2 of this Article;
- b) Mandatory cessation of the provision of telecommunications or Internet services, or disconnection from telecommunications networks or the Internet in Vietnam, in respect of the violation prescribed in Point a Clause 2 of this Article;
- c) Mandatory removal from digital application stores intended for the Vietnamese market, in respect of the violation prescribed in Point a Clause 2 of this Article.

Article 30. Violations of regulations on cooperation with specialized cybersecurity protection force in investigating and handling violations of law

1. A fine ranging from VND 25.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Failing, without a legitimate reason, to provide user information to the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam, or taking more than

24 hours to provide such information, after receiving a written request for the investigation and handling of a violation of the law on cybersecurity;

b) Failing to comply with a request from the specialized cybersecurity protection force of the Ministry of Public Security of Vietnam concerning the management or provision of Internet services to an organization or individual committing a violation prescribed in Clauses 1, 2, or 3 of Article 13 of the Law on Cybersecurity;

c) Failing to implement managerial measures to prevent, detect, block, remove, or delete information containing the content prescribed in Clauses 1, 2, and 3 of Article 13 of the Law on Cybersecurity from an information system under its management at the request of the specialized cybersecurity protection force.

2. Remedial measure: Mandatory implementation of network information security safeguards in accordance with regulations, in respect of the violations prescribed in Clause 1 of this Article.

Article 31. Violations of regulations on protection of children in cyberspace

1. A fine ranging from VND 25.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to implement measures to control information content on a system or service provided by an enterprise that is harmful to children or infringes upon children or children's rights;

b) Failing to prevent the sharing of, or delete, information containing content that is harmful to children or infringes upon children or children's rights;

c) Failing to provide warnings for information technology products or services containing content that is detrimental to children;

d) Failing to implement appropriate measures prescribed by Vietnamese law to ensure the detection, identification, and prevention of children directly creating or using service accounts with their own information;

dd) Failing to develop features in accordance with legal guidance to assist parents or lawful guardians in creating accounts for children using the information of the parents or lawful guardians under the civil law and in managing and supervising the children's activities;

e) Failing to disable or cancel service accounts directly created or used by children after a functional authority has identified such accounts and issued a request in writing or through another agreed appropriate form of communication.

2. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Posting, disseminating, sharing, retaining, exchanging, or using information, images, or audio containing pornographic, depraved, or violent content involving children;

b) Posting, sharing, or disseminating information that insults the honor, reputation, or dignity of children or adversely affects their health or normal physiological or psychological development, where the violation is not serious enough for criminal prosecution.

3. A fine ranging from VND 70.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

a) Failing to cooperate with a competent authority in safeguarding children's rights in cyberspace;

b) Inciting, inducing, enticing, or coercing children to follow, share, or disseminate information containing content that is harmful to children or infringes upon children or children's rights, or to participate in other unlawful activities.

4. Additional penalties:

a) Confiscation of exhibits and means used for committing the administrative violation prescribed in Clause 2 of this Article;

b) Expulsion from the territory of the Socialist Republic of Vietnam of a foreigner committing any of the violations prescribed in Clause 2 of this Article.

5. Remedial measures:

a) Mandatory implementation of measures for protecting children in cyberspace in accordance with regulations, in respect of the violations prescribed in Clause 1 of this Article;

b) Mandatory deletion or correction of information, in respect of the violations prescribed in Clause 2 of this Article;

c) Mandatory revocation of subscriber numbers, prefixes, and telecommunications numbering resources; Internet resources, domain names, Internet Protocol addresses (IP addresses), and autonomous system numbers (ASNs); management codes and service provision numbers; and mandatory return of IP addresses, ASNs, domain names, and digital accounts, in respect of the violations prescribed in Clause 2 of this Article;

d) Mandatory remittance of illegal profits obtained from committing the administrative violations, or mandatory remittance of an amount equal to the value of exhibits or means of administrative violations that have been sold, dispersed, or destroyed, in respect of the violations prescribed in Clause 2 of this Article.

Article 32. Violations of regulations on implementation of cybersecurity protection measures

1. A fine ranging from VND 25.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) An enterprise providing services on telecommunications networks or the Internet or value-added services in cyberspace, or an information system administrator, failing to remove, as prescribed, unlawful or false information in cyberspace that infringes upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, or individuals after receiving a request from the specialized cybersecurity protection force;

b) Failing to suspend or request the cessation of the operation of an information system or revoke a domain name after receiving a request from the specialized cybersecurity protection force.

2. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Clause 1 of this Article.

3. Remedial measures:

a) Mandatory implementation of cybersecurity safeguards, in respect of the violations prescribed in Clause 1 of this Article;

b) Mandatory revocation of the domain name involved in any of the violations prescribed in Clause 1 of this Article.

Article 33. Violations of regulations on data retention and establishment of branches or representative offices in Vietnam

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to retain data or failing to fully retain sensitive national security data as prescribed in the Decree elaborating on the Law on Cybersecurity 2025;

b) Failing to comply with a decision requiring the retention of sensitive national security data or the establishment of a branch or representative office in Vietnam;

c) Failing to retain system logs for the period required for the investigation and handling of violations of the law on cybersecurity as prescribed in Point b Clause 2 of Article 25 of the Law on Cybersecurity 2025.

2. Additional penalty: Expulsion from the territory of the Socialist Republic of Vietnam of a foreigner committing any of the violations prescribed in Clause 1 of this Article.

3. Remedial measures:

a) Mandatory retention of data or establishment of a branch or representative office in Vietnam;

b) Mandatory cessation of the provision of telecommunications or Internet services, or disconnection from telecommunications networks or the Internet in Vietnam, in respect of the violations prescribed in Clause 1 of this Article.

Section 4. VIOLATIONS OF REGULATIONS ON MANAGEMENT OF CYBERSECURITY PRODUCTS AND SERVICES

Article 34. Violations of regulations on authentication, identification, and security of digital accounts

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Failing to authenticate and identify a digital account using lawful identity documents, or authenticating and identifying such account using unlawful documents, where authentication and identification are mandatory under the law;

b) Failing to implement measures to alert the owner when a digital account is used for transactions involving money, finance, securities, or other assets transferable in cyberspace, whether conducted electronically or by another method specified in published internal regulations;

c) Failing to retain information concerning the device, IP address, and login time associated with a digital account for at least 90 days;

d) Failing to suspend transactions or freeze a digital account used for transactions involving money, finance, securities, or other assets transferable in cyberspace upon detecting an error, mistake, or information disclosure or leak, or upon receiving a notification or request from the specialized cybersecurity protection force;

dd) Using electronic identification methods that inaccurately identify the holder of a digital account used for transactions involving money, finance, securities, or other assets transferable in cyberspace;

e) Failing to retain account authentication records or access logs, or failing to establish an anomaly-detection mechanism for a digital account with financial transaction functions.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Using another person's identity documents to authenticate a digital account;

b) Using forged identity documents; creating, altering, editing, or compositing images of identity documents; or employing other fraudulent means to authenticate a digital account;

c) Using artificial intelligence (AI), deepfake technology, or other advanced technological measures to forge biometric data, including facial or voice data, for the purpose of unlawfully authenticating an account.

3. Remedial measure: Mandatory restoration to the original state, in respect of the violations prescribed in Clauses 1 and 2 of this Article.

Article 35. Violations of regulations on business activities in field of cybersecurity

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Failing to manage dossiers and documents concerning the technical and technological solutions of cybersecurity products;
- b) Failing to create and retain records of, or ensure the confidentiality of, information concerning clients using cybersecurity products or services;
- c) Failing to report to the Ministry of Public Security of Vietnam on the business, export, or import of cybersecurity products or services in accordance with regulations.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Failing to carry out procedures for replacement of the license to trade in cybersecurity products or services where the enterprise changes its name or legal representative or changes or supplements the cybersecurity products or services it provides;
- b) Failing to carry out procedures for reissuance of the license where the license to trade in cybersecurity products or services is lost or damaged;
- c) Failing to refuse to provide cybersecurity products or services upon discovering that an organization or individual has violated the law or an agreed undertaking concerning the use of such products or services;
- d) Failing to suspend or cease the provision of cybersecurity products or services at the request of a competent state authority;
- dd) Failing to conduct certification of conformity or declaration of conformity, or failing to use the conformity mark as prescribed, before placing a cybersecurity product on the market;
- e) Providing cybersecurity services inconsistently with the contents specified in the license to trade in cybersecurity products or services.

3. A fine ranging from VND 50.000.000 to VND 75.000.000 shall be imposed for any of the following violations:

- a) Failing to maintain any of the conditions for issuance of a license to trade in cybersecurity products or services;
- b) Failing to cooperate in or facilitate the implementation of professional measures at the request of a competent state authority.

4. A fine ranging from VND 75.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

- a) Trading in cybersecurity products or services without a license;
- b) Trading in cybersecurity products or services in a manner detrimental to national defense, security, or order, where the violation is not serious enough for criminal prosecution;
- c) Providing inaccurate or fabricated information to obtain a license to trade in cybersecurity products or services.

5. Additional penalty: Deprivation of the right to use the license to trade in cybersecurity products or services for a definite period of between 3 and 6 months in respect of the violations prescribed in Points a and e Clause 2 and Point b Clause 4 of this Article.

6. Remedial measure: Mandatory remittance of illegal profits obtained from the violations prescribed in Points c, d, dd and e Clause 2 and in Clause 4 of this Article.

Article 36. Violations of regulations on import of cybersecurity products

1. A fine ranging from VND 75.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

- a) Importing a cybersecurity product included in the list of imports subject to licensing without an import license;
- b) Providing inaccurate or fabricated information to obtain a license to import cybersecurity products.

2. Additional penalty: Deprivation of the right to use the license to trade in cybersecurity products or services for a definite period of between 1 and 3 months in respect of the violations prescribed in Clause 1 of this Article.

3. Remedial measures:

- a) Mandatory remittance of illegal profits obtained from the violations prescribed in Clause 1 of this Article;
- b) Mandatory recall of cybersecurity products, in respect of the violations prescribed in Clause 1 of this Article.

Section 5. VIOLATIONS OF REGULATIONS ON COMBATING SPAM MESSAGES, SPAM EMAILS, AND SPAM CALLS

Article 37. Violations of regulations relating to emails and messages providing information on products and services

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

- a) Sending advertising emails or advertising messages to recipients without their prior consent;
- b) Incorrectly or incompletely labeling advertising emails or advertising messages as prescribed;
- c) Making advertising calls to users without obtaining their explicit prior consent;
- d) Making advertising calls to users who have indicated that they do not consent to receiving advertising calls in client consent records;
- dd) Sending an advertising opt-in message after a user has refused or failed to respond to an advertising opt-in message;
- e) Sending advertising messages to a user who has refused to receive such messages.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Failing to label advertising emails or advertising messages as prescribed;
- b) Failing to retain information concerning subscriptions to advertisements, opt-out requests, and confirmations of requests to opt out of advertising emails, advertising messages, or advertising calls for at least 1 year;
- c) Sending advertising messages or making advertising calls without having been issued an identifier name, or using a telephone number to send advertising messages or make advertising calls.

3. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Failing to provide users, free of charge, with a mechanism for receiving and processing spam reports;
- b) Failing to implement measures to prevent the loss or blocking of emails belonging to service users;

- c) Failing to cooperate with domestic and foreign Internet service providers and messaging service providers in restricting or blocking spam;
- d) Failing to confirm receipt of a request to opt out of emails or messages within the time limit or in the form or with the contents prescribed by law;
- dd) Failing to implement measures limiting the number, transmission speed, or frequency of messages;
- e) Failing to limit the frequency of messages from each sending source or block messages posing risks to information safety or security as prescribed;
- g) Concealing one's name or electronic address when sending emails or messages;
- h) Failing to cooperate with domestic and foreign telecommunications enterprises licensed to establish mobile telecommunications networks in blocking spam messages;
- i) Failing to implement measures to block spam messages at the request of a competent state authority;
- k) Failing to block spam messages with spoofed sending sources before they are delivered to service users;
- l) Failing to cease the provision of content services via messages at a client's request;
- m) Failing to fully comply with requirements for coordinating, blocking, or handling spam messages;
- n) Sending more than 3 advertising messages to 1 telephone number, more than 3 advertising emails to 1 email address, or making more than 1 advertising call to 1 telephone number within a 24-hour period without a different agreement with the user;
- o) Sending advertising messages outside the hours of 07:00 to 10:00 each day, or making advertising calls outside the hours of 08:00 to 17:00 each day, without an agreement with the user;
- p) Failing to implement measures to verify a user's explicit prior consent before sending advertising messages or advertising emails or making advertising calls;
- q) Failing to provide users with tools for searching or retaining agreements concerning subscriptions to, or refusal of, advertising calls or advertising opt-in messages for inspection, examination, and the resolution of complaints and denunciations;
- r) Failing to instruct service users on methods of combating spam messages, spam calls, and spam emails;

s) Failing to comply with the reporting regulations, failing to submit reports in accordance with regulations, or submitting untruthful reports concerning the use of identifier names and/or the prevention and blocking of spam messages and spam calls.

4. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Failing to comply with requirements for coordinating, blocking, or handling spam messages;

b) Failing to comply with a request from the Ministry of Public Security of Vietnam to handle notifications or reports concerning spam messages;

c) Failing to implement measures to restrict spam emails at the request of a competent state authority;

d) Failing to provide information or block sources disseminating spam emails or malware at the request of a competent state authority;

dd) Failing to implement measures for assessing the prevalence of spam messages on the messaging service provider's mobile telecommunications network in accordance with the guidance of the Ministry of Public Security of Vietnam;

e) Making an advertising call without providing complete information concerning the full name and position of the caller and the name and address of the advertising entity before presenting the advertising content, or without providing information concerning charges where fee-based services are advertised.

5. A fine ranging from VND 70.000.000 to VND 80.000.000 shall be imposed for any of the following violations:

a) Failing to provide all prescribed methods for opting out of advertising emails or advertising messages;

b) Sending or disseminating spam emails, spam messages, or malware causing less serious consequences, or making spam calls;

c) Generating missed calls on a mass scale to induce users to call or send messages to content service numbers for profit or for the provision of information or advertisements;

d) Utilizing or using service numbers or telecommunications subscriber numbers for improper purposes;

dd) Enabling outgoing calls or the sending or receipt of messages through toll-free service numbers or premium-rate service numbers;

e) Sending advertising opt-in messages contrary to regulations of the Ministry of Public Security of Vietnam;

g) Sending any advertising opt-in message to a telephone number included in the do-not-advertise list;

h) Failing to retain, or incompletely retaining, advertising call logs, including audio recordings of advertising calls, as prescribed for inspection, examination, supervision, and the resolution of complaints and denunciations.

6. A fine ranging from VND 80.000.000 to VND 90.000.000 shall be imposed for any of the following violations:

a) Conducting advertising by email, message, or call, or providing Internet-based messaging or calling services, without maintaining a system for receiving and processing recipients' opt-out requests;

b) Sending advertising messages or making advertising calls to telephone numbers included in the do-not-advertise list.

7. A fine ranging from VND 90.000.000 to VND 100.000.000 shall be imposed for failing to block or revoke subscriber numbers used to disseminate spam messages or make spam calls.

8. Additional penalties:

a) Suspension of the provision of services to new clients for a definite period of between 1 and 3 months in respect of the violations prescribed in Points c, d, dd, and h Clause 3 and in Clauses 5 and 6 of this Article;

b) Suspension of the right to use an identifier name for a definite period of between 1 and 3 months in respect of the violations prescribed in Points a and b Clause 2; Points d, g, h, I, and o Clause 3; and Points a and b Clause 5 of this Article.

9. Remedial measures:

a) Mandatory return or remittance of illegal profits obtained from the violations prescribed in Points d and dd Clause 5 of this Article;

b) Mandatory revocation of prefixes or telecommunications numbering resources involved in the violations prescribed in Points b and c Clause 4 and in Clause 5 of this Article;

c) Mandatory revocation of telephone numbers involved in the violations prescribed in Clause 1 of this Article.

Article 38. Violations of regulations on provision of advertising email, advertising messaging, advertising calling, and message-based content services

1. A fine ranging from VND 5.000.000 to VND 10.000.000 shall be imposed for any of the following violations:

- a) Failing to maintain a website using a Vietnamese country-code domain name when providing advertising email services, Internet-based messaging services, or message-based content services;
- b) Failing to provide complete and clear information concerning services on the website before providing such services, including the service name, corresponding command code, service description, instructions for use, corresponding service charge, instructions for cancelling the service, customer support telephone number, and confirmation of consent to use the service;
- c) Failing to provide tools or applications enabling users to proactively block and report spam emails;
- d) Failing to implement measures to block and filter spam emails and update the list of sources disseminating spam emails, or failing to implement solutions to prevent the loss or erroneous blocking of users' emails;
- dd) Failing to monitor, control, and scan its email server system to ensure that the system does not become a source of spam emails;
- e) Failing to submit periodic reports or statistics as prescribed by a competent state authority.

2. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

- a) Failing to provide information concerning charges before charging a user who calls a premium-rate call center or information inquiry service;
- b) Failing to instruct subscribers on how to submit spam message reports or respond to received spam message reports;
- c) Incompletely retaining data concerning the provision of message-based content services as prescribed;
- d) Failing to develop, update, provide, or share a common list of IP addresses or domain names disseminating spam emails with the Ministry of Public Security of Vietnam's Department of Cybersecurity and High-Tech Crime Prevention and Control and other telecommunications and Internet enterprises.

3. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Providing information concerning products or services by email through an email server not located in Vietnam;

- b) Providing Internet-based messaging services through a messaging service server not located in Vietnam;
- c) Providing information concerning products or services by message without using a message-sending number allocated in accordance with regulations;
- d) Providing advertising email or advertising messaging services without maintaining a system for receiving and processing requests to opt out of advertising emails or advertising messages;
- dd) Failing to provide, free of charge, a function for receiving users' reports concerning spam messages or spam emails;
- e) Failing to implement a spam-message blocking system capable of blocking spam messages according to the sending source or keywords contained in the messages;
- g) Failing to permit an enterprise issued a management code to establish a technical connection to its system for service provision;
- h) Failing to retain data concerning the provision of message-based content services as prescribed;
- i) Failing to provide users with tools or applications for reporting spam messages or spam calls and proactively blocking spam messages or spam calls;
- k) Failing to provide, update, or share common spam-message templates with the Ministry of Public Security of Vietnam's Department of Cybersecurity and High-Tech Crime Prevention and Control and other telecommunications enterprises;
- l) Failing to block or filter IP addresses or domain names under its management that disseminate, or are misused to disseminate, spam emails;
- m) Failing to implement measures for assessing the prevalence of spam messages or spam calls on its telecommunications network;
- n) Using an identifier name that was not issued by the Ministry of Public Security of Vietnam's Department of Cybersecurity and High-Tech Crime Prevention and Control, was issued by that Department to another organization or individual, or has been revoked;
- o) Using an identifier name to send spam messages, make spam calls, or provide services in violation of the law, as concluded by a state authority.

4. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Charging service fees for erroneous messages, messages for which no service was provided, messages for which the provided content differed from the command code published by the enterprise, or messages sent because users were deceived;
- b) Failing to implement measures to prevent advertising messages or advertising calls from being sent or made to telephone numbers included in the do-not-advertise list;
- c) Failing to block or revoke electronic addresses used to disseminate spam messages, spam emails, or spam calls at the request of a competent state authority;
- d) Failing to develop and operate a technical system for preventing and blocking spam messages, spam emails, and spam calls;
- dd) Failing to develop its identifier name management system or connect such system to the National Identifier Name Management System;
- e) Failing to perform tasks involving the coordination, blocking, and handling of spam emails or spam calls or other professional measures at the request of the Ministry of Public Security of Vietnam's Department of Cybersecurity and High-Tech Crime Prevention and Control.

5. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed on a telecommunications enterprise providing Voice over Internet Protocol (VoIP) or SIP Trunk services for any of the following violations:

- a) Failing to implement or maintain a technical mechanism for automatically blocking all SIP Trunk or VoIP traffic that generates outgoing calls to the public telecommunications network without a valid identifier name (Voice Brandname) as prescribed;
- b) Failing to monitor, analyze, or detect abnormal call traffic according to technical criteria promulgated or provided by a competent state authority;
- c) Failing to implement, or incompletely implementing, measures to warn, restrict, suspend, or terminate the provision of services to clients showing signs of generating spam, fraudulent, or impersonation calls, as requested by a competent authority or indicated by internal monitoring results;
- d) Failing to retain or promptly provide logs, technical data, or identification information relating to SIP Trunk or VoIP traffic for inspection, examination, investigation, or verification in accordance with the law.

6. Additional penalties:

- a) Suspension of the provision of services to new clients for a definite period of between 1 and 3 months in respect of the violations prescribed in Clause 4 of this Article;

b) Suspension of the provision of SIP Trunk or VoIP services for a definite period of between 1 and 3 months in respect of a telecommunications enterprise committing any of the violations prescribed in Clause 5 of this Article.

7. Remedial measure: Mandatory revocation of the identifier name involved in any of the violations prescribed in Clause 4 of this Article.

Section 6. VIOLATIONS OF REGULATIONS ON PERSONAL DATA PROTECTION

Article 39. Violations of regulations on personal data protection principles and prohibited acts

1. A fine ranging from VND 20.000.000 to VND 40.000.000 shall be imposed for any of the following violations:

- a) Processing personal data beyond the determined scope, inconsistently with the personal data processing purposes for which consent was sought or an agreement was reached, or beyond the extent necessary to achieve such purposes;
- b) Failing to ensure the accuracy of personal data, or failing to promptly rectify, update, or supplement such data upon detecting errors or where necessary;
- c) Retaining personal data beyond the period necessary for the relevant personal data processing purposes, unless otherwise prescribed by law;
- d) Failing to proactively prevent or detect violations, or to promptly cooperate with competent authorities in handling any violation of the law on personal data protection.

2. A fine ranging from VND 40.000.000 to VND 60.000.000 shall be imposed for any of the following violations:

- a) Resisting or obstructing personal data protection activities of agencies, organizations, or individuals;
- b) Using another person's personal data to commit acts contrary to the law.

3. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Points a and c Clause 1 and Point b Clause 2 of this Article.

4. Remedial measures:

- a) Mandatory destruction or irreversible deletion of personal data processed beyond the permitted scope, for improper purposes, or retained beyond the prescribed period, in respect of the violations prescribed in Points a and c Clause 1 of this Article;

- b) Mandatory remittance of illegal proceeds obtained from the violations prescribed in Points a and c Clause 1 and Point b Clause 2 of this Article;
- c) Mandatory public apology to the data subject through mass media in respect of the violation prescribed in Point b Clause 2 of this Article;
- d) Mandatory rectification, updating, or supplementation of personal data to ensure its accuracy at the request of the data subject or upon detecting errors, in respect of the violation prescribed in Point b Clause 1 of this Article.

Article 40. Violations involving misuse of personal data protection activities to commit unlawful acts

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following acts involving the misuse of personal data protection activities:

- a) Using the guise of personal data protection activities to conceal, legitimize, or facilitate an unlawful act;
- b) Misusing the deployment of forces, equipment, or measures to prevent and combat infringements of personal data to appropriate, falsify, or unlawfully process personal data;
- c) Using personal data protection activities to commit fraudulent acts or infringe upon the lawful rights and interests of agencies, organizations, or individuals.

2. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Clause 1 of this Article.

3. Remedial measures:

- a) Mandatory destruction or irreversible deletion of personal data that has been appropriated or unlawfully processed in respect of the violations prescribed in Clause 1 of this Article;
- b) Mandatory remittance of illegal proceeds obtained from the violations prescribed in Clause 1 of this Article;
- c) Mandatory public apology to the data subject through mass media in respect of the violations prescribed at Points b and c Clause 1 of this Article.

Article 41. Violations of regulations on personal data processing affecting security and order

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following acts of personal data processing affecting security and order:

- a) Processing personal data to create, reinforce, or disseminate fabricated, false, distorted, or inflammatory information that causes public anxiety or affects security and order;
- b) Providing, transferring, disseminating, or disclosing personal data while knowing that such data will be used for purposes that infringe upon security and order;
- c) Modifying, falsifying, deleting, destroying, or appropriating personal data, or interrupting personal data processing, with the aim of disrupting the normal operations of agencies or organizations;
- d) Committing other acts that affect or pose a risk of affecting security and order.

2. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Clause 1 of this Article.

3. Remedial measures:

- a) Mandatory destruction or irreversible deletion of personal data processed for the purpose of affecting security and order in respect of the violations prescribed in Clause 1 of this Article;
- b) Mandatory remittance of illegal proceeds obtained from the violations prescribed in Clause 1 of this Article;
- c) Mandatory removal or withdrawal of information and personal data unlawfully provided, transferred, or disclosed in respect of the violation prescribed in Point b Clause 1 of this Article.

Article 42. Violations by data subjects of personal data protection obligations

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

- a) Intentionally disclosing or losing their own personal data, thereby affecting social order and safety or causing damage to relevant agencies, organizations, or individuals;
- b) Intentionally allowing another person to use their personal data to commit acts contrary to the law;
- c) Intentionally providing forged or false personal data for the purpose of defrauding or misleading relevant agencies, organizations, or individuals;
- d) Intentionally fabricating an incident involving the disclosure or loss of their own personal data to evade liability, claim compensation, or seek illegal profits, thereby adversely affecting the reputation or property of other organizations or individuals;

dd) Intentionally failing to fully and accurately provide their personal data as mandatorily required by law or under a concluded contract, thereby creating risks relating to legal identification or causing financial damage to the data processing and controlling party.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed on an individual who commits any of the following violations:

- a) Unlawfully collecting, using, disclosing, modifying, falsifying, destroying, or accessing another person's personal data, thereby causing damage to that person's lawful rights and interests;
- b) Intentionally providing another person's personal data for the purpose of defrauding or misleading relevant agencies, organizations, or individuals;
- c) Abusing the exercise of data subject rights beyond the extent necessary or inconsistently with the purposes for which such rights are exercised, thereby causing difficulties for or obstructing the lawful business operations of agencies or organizations;
- d) Refusing to cooperate in preventing and combating infringements of personal data upon receiving an official request from a competent state authority.

3. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Clauses 2 and 3 of this Article.

4. Remedial measures:

- a) Mandatory destruction or irreversible deletion of another person's personal data that has been unlawfully collected in respect of the violation prescribed in Point a Clause 2 of this Article;
- b) Mandatory remittance of illegal proceeds obtained from the violations prescribed in Points b and c Clause 2 of this Article;
- c) Mandatory re-provision of accurate and complete personal data as prescribed by law or under the relevant contract in respect of the violation prescribed in Point dd Clause 1 of this Article;
- d) Mandatory cessation of acts obstructing the lawful exercise of rights and performance of obligations relating to personal data processing in respect of the violation prescribed in Point c Clause 2 of this Article.

Article 43. Violations of regulations on data subjects' consent

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Processing personal data after its collection without obtaining the data subject's consent, unless otherwise prescribed by law;

b) Imposing a mandatory condition or refusing to provide services where the data subject does not consent to the processing of personal data for purposes unrelated to the relevant service provision agreement;

c) Establishing consent by default or providing unclear or misleading instructions regarding whether the data subject consents or does not consent;

d) Failing to obtain consent in a clear and specific manner, or failing to ensure that the identity of the data subject giving consent and the time and contents of such consent can be verified;

dd) Failing to provide the data subject with transparent information on the types of personal data to be processed, the personal data processing purposes, or the rights and obligations of the data subject, the personal data controlling party, or the personal data processing and controlling party, thereby resulting in consent that is not freely and knowingly given;

e) Using a form of obtaining consent that does not allow the data subject to consent separately to each personal data processing purpose;

g) Failing to record or retain logs of the data subject's consent, or failing to prove that consent has been obtained upon request of the data subject or upon a request for inspection or examination by a competent state authority;

h) Failing to notify the data subject that their sensitive personal data is being processed.

2. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Intentionally continuing to process personal data after the data subject has requested the cessation or restriction of processing, or after a competent state authority has made such a request in writing;

b) Collecting or processing personal data where the data subject remains silent or does not respond to a request for consent, and unilaterally treating such silence as consent.

3. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Points a and c Clause 1 and Clause 2 of this Article.

4. Remedial measures:

a) Mandatory destruction or irreversible deletion of personal data collected or processed without valid consent in respect of the violations prescribed in Points a and c Clause 1 and Clause 2 of this Article;

b) Mandatory remittance of illegal proceeds obtained from the violations prescribed in Clause 2 of this Article.

Article 44. Violations of regulations on procedures for exercising data subject rights

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed on a personal data controlling party or a personal data processing and controlling party that commits any of the following violations:

- a) Failing to establish clear processes, procedures, and forms for the exercise of data subject rights;
- b) Failing to clearly assign responsibilities among relevant units within the organization for facilitating the exercise of data subject rights;
- c) Failing to provide information or ensure that the data subject is informed of the procedures for exercising the rights prescribed in the Law on Personal Data Protection;
- d) Failing to respond to the data subject, or failing to provide complete information on the applicable procedures, within 2 working days from the receipt of a valid request to view, rectify, obtain, or delete personal data; withdraw consent; restrict or object to personal data processing; or have personal data protection measures and solutions implemented;
- dd) Failing to notify the data subject of legitimate reasons, where a request cannot be fulfilled or requires an extension, including a request to view, rectify, obtain, or delete personal data; withdraw consent; restrict or object to personal data processing; or have personal data protection measures and solutions implemented.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed on a personal data processing party or a third party that has received a valid request from a personal data controlling party or a personal data processing and controlling party but fails to fulfill any of the following requests within the specified period:

- a) Failing to cease personal data processing, upon receiving a request for withdrawal of consent, restriction of processing, or objection to personal data processing, within the period specified by the personal data controlling party or the personal data processing and controlling party;
- b) Failing to rectify or provide personal data within the period specified by the personal data controlling party or the personal data processing and controlling party;
- c) Failing to delete or destroy personal data, or to restrict personal data processing, within the period specified by the personal data controlling party or the personal data processing and controlling party.

3. A fine ranging from VND 30.000.000 to VND 40.000.000 shall be imposed on a personal data controlling party or a personal data processing and controlling party that fails to fulfill any of the following requests of a data subject within the prescribed period:

a) Failing to fulfill a request for withdrawal of consent, restriction of processing, or objection to personal data processing within 15 days; failing to ensure fulfillment within 20 days where it is necessary to request a personal data processing party or a third party to do so; or, where an extension has been granted, failing to ensure fulfillment within the extended period of up to 15 days;

b) Failing to fulfill a request to view, rectify, or obtain personal data within 10 days; failing to ensure fulfillment within 15 days where it is necessary to request a personal data processing party or a third party to do so; or, where an extension has been granted, failing to ensure fulfillment within the extended period of up to 10 days;

c) Failing to fulfill a request for deletion of personal data within 20 days; failing to ensure fulfillment within 30 days where it is necessary to request a personal data processing party or a third party to do so; or, where an extension has been granted, failing to ensure fulfillment within the extended period of up to 20 days;

d) Failing to fulfill a request for the implementation of personal data protection measures and solutions within 15 days or, where an extension has been granted, failing to ensure fulfillment within the extended period of up to 15 days.

4. A personal data processing party or a third party shall not be penalized under Clause 2 of this Article where otherwise prescribed by law.

5. Remedial measures: Mandatory full fulfillment of data subject rights in accordance with lawful requests and provision of evidence of such fulfillment to the competent authority in respect of the violations prescribed in Clauses 2 and 3 of this Article.

Article 45. Violations of regulations on right to withdraw consent and right to restrict personal data processing

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Employing methods or measures to conceal, prevent, or deliberately obstruct a data subject's exercise of the right to withdraw consent or request restriction of processing;

b) Failing to cease personal data processing after the data subject has duly withdrawn consent or requested restriction of processing, except where continued processing without consent is permitted under Article 19 of the Law on Personal Data Protection;

c) A personal data controlling party or a personal data processing and controlling party failing to request a personal data processing party or a third party to cease processing the personal data of a data subject who has withdrawn consent or requested restriction of personal data processing.

2. Remedial measures:

- a) Mandatory destruction or irreversible deletion of personal data that continued to be processed after the data subject had withdrawn consent, in respect of the violation prescribed in Point b Clause 1 of this Article;
- b) Mandatory remittance of proceeds obtained from the continued utilization of personal data after the data subject had withdrawn consent, in respect of the violation prescribed in Point b Clause 1 of this Article;
- c) Mandatory establishment and provision to the data subject of a clear and readily accessible technical mechanism for exercising the right to withdraw consent, and provision of evidence of implementation to the competent authority, in respect of the violation prescribed in Point a Clause 1 of this Article;
- d) Mandatory submission of a request to the personal data processing party or the third party to cease processing the personal data of the data subject who has withdrawn consent, and provision of evidence of implementation, in respect of the violation prescribed in Point c Clause 1 of this Article.

Article 46. Violations of regulations on right to view or rectify personal data or request its rectification

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) A personal data controlling party or a personal data processing and controlling party refusing or failing to allow a data subject to access and view or rectify their personal data, or request its rectification, after such data has been collected, unless otherwise prescribed by law;
- b) A personal data processing party or a third party modifying a data subject's personal data on its own initiative without the prior written approval of the data controller.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for deliberately delaying or failing to rectify personal data after confirming that the information is false or forged and adversely affects the honor, dignity, reputation, or lawful rights and interests of the data subject.

3. No penalty under this Article shall be imposed for refusing or not yet rectifying personal data where the personal data controlling party or the personal data processing and controlling party has reasonable grounds to demonstrate that the case falls into any of the following cases:

- a) The request for rectification is intended to facilitate fraud, falsify information to evade a legal obligation, or commit an unlawful act;
- b) Rectification of personal data as requested may infringe upon the lawful rights and interests of another organization or individual, or adversely affect fine traditions and customs, morality, or the public interest;

c) Other cases prescribed by relevant laws.

4. Remedial measures:

a) Mandatory rectification of personal data in accordance with the lawful request of the data subject, in respect of the violation prescribed in Clause 2 of this Article;

b) Mandatory destruction or irreversible deletion of personal data that has been modified on one's own initiative and unlawfully, in respect of the violation prescribed in Point b Clause 1 of this Article.

Article 47. Violations of regulations on personal data processing without data subject consent

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

a) Failing to establish processes and rules for personal data processing and determine the responsibilities of agencies, organizations, and individuals during personal data processing;

b) Failing to periodically inspect and assess compliance with the law and with processes and rules for personal data processing;

c) Failing to establish a mechanism for receiving and handling feedback and recommendations from relevant agencies, organizations, and individuals.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Failing to implement appropriate personal data protection measures, resulting in the disclosure or loss of collected personal data;

b) Failing to assess risks that may arise during personal data processing.

3. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Abusing the cases in which personal data may be processed without consent, as prescribed in Clause 1 Article 19 of the Law on Personal Data Protection, to collect or process personal data beyond the purposes or scope necessary under the applicable legal grounds;

b) Failing to demonstrate that the processing of personal data without consent falls within a case prescribed by law upon an inspection request from a competent state authority.

4. Remedial measures:

- a) Mandatory establishment, promulgation, and publication of processes and rules for personal data processing, personal data protection measures, and a mechanism for receiving feedback and recommendations in accordance with regulations, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 1 of this Article;
- b) Mandatory cessation of personal data processing conducted on the basis of an improperly invoked consent exemption, or beyond the purposes or scope permitted by such legal grounds, in respect of the violations prescribed in Clause 3 of this Article;
- c) Mandatory destruction or irreversible deletion of all personal data collected or processed beyond the prescribed purposes or scope or without lawful grounds, in respect of the violation prescribed in Point a Clause 3 of this Article;
- d) Mandatory preparation, retention, and provision of documents demonstrating the lawful grounds for personal data processing without consent, upon request of a competent authority, in respect of the violation prescribed in Point b Clause 3 of this Article;
- dd) Mandatory implementation of appropriate personal data protection measures and performance of a risk assessment during personal data processing, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 2 of this Article.

Article 48. Violations of regulations on personal data collection

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for collecting personal data beyond the permitted scope, for purposes that are not specific and clear, or without obtaining the data subject's consent prior to collection as prescribed by law.
2. A fine ranging from VND 50.000.000 to VND 80.000.000 shall be imposed for collecting or retaining personal data, or creating personal data repositories from personal data transfer activities, for use for purposes other than those to which the data subject has consented.
3. Where technological or technical measures are employed to collect personal data contrary to the law, the fines shall be determined as follows:
 - a) A fine ranging from VND 100.000.000 to VND 200.000.000 for collecting basic personal data of fewer than 500 data subjects, or sensitive personal data of fewer than 100 data subjects;
 - b) A fine ranging from VND 200.000.000 to VND 300.000.000 for collecting basic personal data of between 500 and fewer than 1.000 data subjects, or sensitive personal data of between 100 and fewer than 200 data subjects;
 - c) A fine ranging from VND 300.000.000 to VND 500.000.000 for collecting basic personal data of between 1.000 and fewer than 5.000 data subjects, or sensitive personal data of between 200 and 1.000 data subjects;

d) A fine ranging from VND 500.000.000 to VND 800.000.000 for collecting basic personal data of 5.000 or more data subjects, or sensitive personal data of 1.000 or more data subjects.

4. A fine ranging from VND 50.000.000 to VND 80.000.000 shall be imposed for the violation prescribed in Clause 1 of this Article where the subject matter of the violation is sensitive personal data.

5. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Clauses 1, 2, and 3 of this Article.

6. Remedial measures:

a) Mandatory destruction or irreversible deletion of all personal data collected or processed contrary to regulations in respect of the violations prescribed in this Article;

b) Mandatory remittance of proceeds obtained from business activities involving the use of unlawfully collected personal data, in respect of the violation prescribed in Clause 2 of this Article.

Article 49. Violations of regulations on provision of personal data

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for refusing to provide a data subject with their own personal data upon receipt of a valid request.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for providing personal data to another agency, organization, or individual without the data subject's consent, unless otherwise prescribed by law.

3. A fine equal to twice the fine prescribed in Clauses 2 and 3 of this Article shall be imposed for providing sensitive personal data.

4. Remedial measures:

a) Mandatory provision of the data subject's personal data to that data subject in accordance with their valid request, in respect of the violation prescribed in Clause 1 of this Article;

b) Mandatory retrieval of personal data provided contrary to regulations, in respect of the violations prescribed in Clauses 2 and 3 of this Article;

c) Mandatory remittance of proceeds obtained from the violation prescribed in Clause 2 of this Article.

Article 50. Violations of regulations on public disclosure of personal data

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Publicly disclosing personal data without a specific purpose or in cases where such public disclosure is not permitted by law;
- b) Publicly disclosing personal data beyond the scope or categories necessary for the purpose of such public disclosure;
- c) Publicly disclosing personal data that does not accurately reflect the data from the original source;
- d) Failing to strictly control and monitor the public disclosure of personal data to ensure compliance with its purposes and scope and with the law;
- dd) Failing to adopt measures to prevent unauthorized access, use, disclosure, copying, modification, deletion, or destruction, or other unlawful processing of publicly disclosed data.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Publicly disclosing personal data, thereby infringing upon the lawful rights and interests of the data subject;
- b) Publicly disclosing personal data without the data subject's consent, except where permitted by law.

3. Remedial measures:

- a) Mandatory correction of information in respect of the violation prescribed in Point c Clause 1 of this Article;
- b) Mandatory removal or retrieval of publicly disclosed personal data in respect of the violations prescribed in Clause 2 of this Article;
- c) Mandatory implementation of measures to control, monitor, and secure personal data that is being publicly disclosed, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Points d and dd Clause 1 of this Article;
- d) Mandatory removal or retrieval of personal data publicly disclosed without a specific purpose or beyond the necessary scope, in respect of the violations prescribed in Points a and b Clause 1 of this Article.

Article 51. Violations of regulations on deletion, destruction, and de-identification of personal data

1. A fine ranging from VND 10.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Failing to notify the data subject of the reasons why their personal data cannot be deleted or destroyed after receiving a request;

b) Failing to delete or destroy personal data using secure measures;

c) Failing to adopt measures to prevent unauthorized intrusion into and recovery of deleted or destroyed data;

d) Failing to strictly control and monitor the de-identification of personal data;

dd) Failing to adopt measures to prevent unauthorized access, copying, appropriation, disclosure, or loss of data during de-identification.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to delete or destroy personal data in the cases prescribed by law;

b) A personal data controlling party or personal data processing and controlling party failing to request a personal data processing party or a third party to delete or destroy the data subject's personal data as prescribed by law;

c) A personal data processing party failing to delete or return all personal data to the personal data controlling party upon termination of the personal data processing contract or agreement;

d) Allowing unauthorized access, copying, appropriation, disclosure, or loss of personal data during de-identification.

3. A fine ranging from VND 50.000.000 to VND 60.000.000 shall be imposed for any of the following violations:

a) Intentionally and unlawfully recovering personal data that has been deleted or destroyed;

b) Re-identifying personal data after it has been de-identified, unless otherwise prescribed by law.

4. Remedial measures:

a) Mandatory destruction or irreversible deletion of personal data in respect of the violations prescribed in Points a and b Clause 2 of this Article;

b) Mandatory notification to the data subject that deletion or destruction cannot be performed in the cases prescribed in Point a Clause 1 of this Article;

c) Mandatory destruction or irreversible deletion of re-identification results and personal data that has been unlawfully recovered, in respect of the violations prescribed in Clause 3 of this Article;

d) Mandatory implementation of measures to control, monitor, and prevent unauthorized access during de-identification, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Points d and dd Clause 1 of this Article.

Article 52. Violations of regulations on personal data transfer

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Entering into a personal data transfer agreement that fails to specify responsibilities for protecting personal data during its transfer and processing; responsibilities for facilitating the exercise of data subject rights; or the responsibilities of the parties to cooperate and ensure compliance upon detecting a violation of personal data protection regulations;

b) Where personal data is shared among units within the same agency or organization for processing in accordance with the established processing purposes, the agency or organization fails to establish a process for controlling the sharing and use of personal data in accordance with regulations, or fails to adopt measures to prevent its internal personnel from unlawfully sharing personal data with a third party.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for transferring personal data as prescribed in Points a and d Clause 1 Article 17 of the Law on Personal Data Protection for a fee to provide services to the data subject or serve the data subject's lawful interests, where any of the following obligations is breached:

a) Failing to clearly determine the roles of the personal data controlling party, personal data processing party, and third party in the personal data transfer;

b) Failing to determine and limit the categories of personal data transferred to those necessary for the transfer purposes;

c) Failing to determine a personal data retention period appropriate to the transfer purposes, or failing to delete or destroy personal data upon fulfillment of such purposes as prescribed by law.

3. A fine ranging from VND 50.000.000 to VND 80.000.000 shall be imposed for transferring sensitive personal data without implementing physical security measures for storage and transmission devices, encryption measures, personal data anonymization, or other security measures during the transfer.

4. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Clause 2 of this Article.

5. Remedial measures:

- a) Mandatory supplementation and completion of the personal data transfer agreement in accordance with regulations, and provision of evidence thereof to the competent authority, in respect of the violations prescribed in Clause 1 of this Article;
- b) Mandatory implementation of prescribed security measures for sensitive personal data being retained and transmitted, in respect of the violation prescribed in Clause 3 of this Article;
- c) Mandatory destruction or irreversible deletion of transferred sensitive personal data where its security cannot be ensured as prescribed, in respect of the violations prescribed in Clauses 2 and 3 of this Article.

Article 53. Violations of regulations on unlawful purchase and sale of personal data

1. A fine ranging from twice to no more than 10 times the proceeds obtained shall be imposed for any of the following acts involving the unlawful purchase or sale of personal data:

- a) Providing, sharing, or exchanging personal data for the purpose of obtaining property or other benefits, where such activity does not fall within any of the cases prescribed in Clause 1 Article 17 of the Law on Personal Data Protection;
- b) Transferring personal data for a fee or other material benefit without a personal data transfer agreement;
- c) Transferring personal data for a fee or other material benefit where the personal data transfer agreement fails to specify the purposes of the transfer, or where the transfer is not conducted in accordance with the purposes specified in such agreement;
- d) Transferring personal data for a fee or other material benefit without establishing a technical system and transparent mechanism enabling the data subject to give precise and clear consent to each transfer based on accurate information concerning the transfer purposes and the organizations or individuals receiving and processing the personal data;
- dd) Transferring personal data for a fee or other material benefit where the personal data is not processed in accordance with the transfer purposes to which the data subject has consented and which are consistent with the registered business lines;
- e) Transferring personal data for a fee or other material benefit without de-identifying the personal data when conducting transactions on a data exchange.

2. Where the violations prescribed in Clause 1 of this Article yield no proceeds and the maximum fine equal to 10 times the proceeds obtained from the violation is less than VND 3.000.000.000, the fine shall be determined up to the maximum fine bracket of VND 3.000.000.000.

3. Where no proceeds are obtained from a violation prescribed in Clause 1 of this Article, the fines shall be determined as follows:

- a) A fine ranging from VND 70.000.000 to VND 100.000.000 for purchasing or selling basic personal data of fewer than 1.000 data subjects, or purchasing or selling sensitive personal data of fewer than 200 data subjects;
- b) A fine ranging from VND 100.000.000 to VND 300.000.000 for purchasing or selling basic personal data of between 1.000 and fewer than 2.000 data subjects, or purchasing or selling sensitive personal data of between 200 and fewer than 400 data subjects;
- c) A fine ranging from VND 300.000.000 to VND 500.000.000 for purchasing or selling basic personal data of between 2.000 and fewer than 10.000 data subjects, or sensitive personal data of between 400 and 2.000 data subjects;
- d) A fine ranging from VND 500.000.000 to VND 1.000.000.000 for purchasing or selling basic personal data of 10.000 or more data subjects, or sensitive personal data of 2.000 or more data subjects;
- dd) A fine ranging from VND 1.000.000.000 to a maximum of VND 3.000.000.000 for unlawfully purchasing or selling personal data, thereby infringing upon national defense, security and order, foreign affairs, or the macroeconomy; the life, health, honor, dignity, or property of data subjects; or the lawful rights and interests of organizations or individuals.

4. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in this Article.

5. Remedial measures:

- a) Mandatory destruction or irreversible deletion, from all storage systems, of all personal data unlawfully purchased or sold in respect of the violations prescribed in this Article;
- b) Mandatory remittance of proceeds obtained from the violations prescribed in Clauses 1 and 2 of this Article;
- c) Mandatory notification to all affected data subjects of the violation and the remedial measures taken in respect of the violations prescribed in this Article.

Article 54. Violations of regulations on notification of violations of personal data protection regulations

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

- a) A personal data processing party detecting a violation but failing to promptly notify the personal data controlling party or the personal data processing and controlling party;

b) A personal data controlling party or personal data processing and controlling party failing to prepare a written record confirming the occurrence of a violation of personal data protection regulations;

c) A personal data controlling party, personal data processing and controlling party, or personal data processing party, when submitting a report on a violation or data leakage incident to the specialized personal data protection authority, deliberately concealing or providing false information concerning the nature or scale of the incident, the categories of personal data involved, or the number of affected data subjects.

2. A fine ranging from VND 20.000.000 to VND 40.000.000 shall be imposed for failing to notify the specialized personal data protection authority in any of the following cases:

a) A violation of personal data protection regulations is detected;

b) Personal data is processed for improper purposes or inconsistently with the relevant agreement;

c) Data subject rights are not ensured or are improperly fulfilled.

3. A fine ranging from VND 40.000.000 to VND 60.000.000 shall be imposed on a personal data controlling party, a personal data processing and controlling party, or a third party that notifies the specialized personal data protection authority later than 72 hours after detecting a violation of personal data protection regulations that causes or may cause harm to national defense, national security, or social order and safety, or infringes upon the life, health, honor, dignity, or property of a data subject.

4. A fine ranging from VND 60.000.000 to VND 80.000.000 shall be imposed for any of the following violations:

a) Failing to implement measures to prevent the violation or remedy its consequences;

b) Failing to cooperate with the specialized personal data protection authority in handling the violation.

5. Remedial measures:

a) Mandatory full performance of the obligation to notify the violation in accordance with the prescribed contents, form, and time limit, and provision of evidence of such performance to the competent authority, in respect of the violations prescribed in Clauses 1, 2, and 3 of this Article;

b) Mandatory implementation of measures to prevent the violation and remedy its consequences as requested by the specialized personal data protection authority, in respect of the violation prescribed in Point a Clause 4 of this Article.

Article 55. Violations of regulations on personal data processing impact assessments

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

- a) Commencing personal data processing activities without preparing or maintaining a personal data processing impact assessment dossier at the enterprise's head office as prescribed in Article 21 of the Law on Personal Data Protection;
- b) Failing to submit 1 original of the personal data processing impact assessment dossier, using the form prescribed in the Appendix to Decree No. 356/2025/ND-CP, to the Department of Cybersecurity and High-Tech Crime Prevention and Control of the Ministry of Public Security of Vietnam within 60 days from the first day on which personal data processing is conducted;
- c) Deliberately failing to complete the impact assessment dossier as requested by the specialized authority where the dossier is incomplete or fails to comply with regulations;
- d) Failing to update the personal data processing impact assessment dossier every 6 months when a change occurs as prescribed by law;
- dd) Failing to update the dossier within 10 days in any case where an update is required by law.

2. A fine ranging from VND 50.000.000 to VND 100.000.000 shall be imposed for deliberately falsifying figures or providing false information in a personal data processing impact assessment dossier, or refusing to rectify or complete the dossier after receiving a written request for remedial action from the Department of Cybersecurity and High-Tech Crime Prevention and Control of the Ministry of Public Security of Vietnam.

3. Remedial measures:

- a) Mandatory preparation, completion, and submission of the personal data processing impact assessment dossier in accordance with regulations, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 1 of this Article;
- b) Mandatory suspension of personal data processing activities until the obligation to submit the personal data processing impact assessment dossier has been fully fulfilled and confirmation has been obtained from the specialized personal data protection authority, in respect of the violation prescribed in Point a Clause 1 of this Article.

Article 56. Violations of regulations on cross-border personal data transfers

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Failing to prepare a cross-border personal data transfer impact assessment dossier before or during the transfer;

- b) Failing to submit 1 original of the cross-border personal data transfer impact assessment dossier to the specialized personal data protection authority within 60 days from the first day on which the transfer is conducted;
- c) Failing to complete the cross-border personal data transfer impact assessment dossier within 30 days after receiving a request from the specialized personal data protection authority;
- d) Failing to periodically update, or otherwise update, the cross-border personal data transfer impact assessment dossier when a change occurs as prescribed by law;
- dd) Failing to keep the cross-border personal data transfer impact assessment dossier readily available for inspection by the specialized personal data protection authority;
- e) Failing to provide notification of the information and contact details of the organization or individual responsible for personal data protection on the data recipient's side after completing the cross-border personal data transfer;
- g) Failing to establish a control mechanism or require the cross-border data recipient to comply with applicable procedures when onward-transferring personal data to another third party, thereby resulting in the personal data of Vietnamese citizens being processed beyond the scope declared in the impact assessment dossier.

2. A fine ranging from VND 50.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

- a) Failing to enter into a contract or transfer instrument binding the cross-border data transferor and recipient to their respective personal data protection responsibilities, or failing to clearly determine responsibility for facilitating the exercise of data subject rights after the data has been transferred;
- b) Failing to obtain the data subject's consent to the purposes of the cross-border personal data transfer, or failing to notify the data subject that their data is being transferred abroad and of the organization receiving the data and the processing purposes;
- c) Failing to implement appropriate security measures during the cross-border personal data transfer, or failing to establish a plan to ensure personal data security after the transfer;
- d) Failing to cooperate in, or obstructing, an inspection by the specialized personal data protection authority of cross-border personal data transfer activities;
- dd) Continuing to conduct cross-border personal data transfers after the specialized personal data protection authority has issued a decision requiring the cessation of such transfers;
- e) Failing to notify the specialized personal data protection authority and failing to require the cross-border data recipient to cease processing and prevent damage upon detecting that the

recipient has committed a violation of personal data protection regulations or that an incident involving the disclosure or loss of personal data has occurred.

3. A fine calculated as a percentage of the organization's total revenue generated in the Vietnamese market during the immediately preceding fiscal year shall be imposed on an organization that conducts a cross-border personal data transfer without preparing an impact assessment dossier, conceals or falsely declares data flows resulting in the disclosure or loss of personal data, or continues transferring data after the specialized personal data protection authority has issued a decision requiring cessation of the transfer. The fines shall be determined as follows:

a) A fine equal to between 1% and 2% of revenue for a violation resulting in the disclosure or loss of personal data of between 10.000 and fewer than 100.000 data subjects who are Vietnamese citizens;

b) A fine equal to between 2% and 3% of revenue for a violation resulting in the disclosure or loss of personal data of between 100.000 and fewer than 1.000.000 data subjects who are Vietnamese citizens;

c) A fine equal to between 3% and 5% of revenue for a violation resulting in the disclosure or loss of personal data of 1.000.000 or more data subjects who are Vietnamese citizens, or for conducting a cross-border personal data transfer after the specialized personal data protection authority has issued a decision requiring cessation of the transfer, thereby causing harm to national defense or national security.

4. Where an organization committing a violation prescribed in Clause 3 of this Article generated no revenue in the Vietnamese market during the immediately preceding fiscal year, or where the fine calculated as a percentage of revenue under the relevant Point is lower than VND 3.000.000.000, the following fines shall apply:

a) A fine ranging from VND 200.000.000 to VND 500.000.000 for a violation resulting in the disclosure or loss of personal data of between 10.000 and fewer than 100.000 data subjects who are Vietnamese citizens;

b) A fine ranging from VND 500.000.000 to VND 1.000.000.000 for a violation resulting in the disclosure or loss of personal data of between 100.000 and fewer than 1.000.000 data subjects who are Vietnamese citizens;

c) A fine ranging from VND 1.000.000.000 to VND 3.000.000.000 for a violation resulting in the disclosure or loss of personal data of 1.000.000 or more data subjects who are Vietnamese citizens, or for conducting a cross-border personal data transfer after the specialized personal data protection authority has issued a decision requiring cessation of the transfer, thereby causing harm to national defense or national security.

5. Additional penalties:

- a) Confiscation of exhibits and means used for committing the administrative violations prescribed in Clauses 2 and 3 of this Article;
- b) Suspension of cross-border personal data transfer activities for a definite period of between 6 and 12 months in respect of the violations prescribed in Clause 3 of this Article.

6. Remedial measures:

- a) Mandatory preparation, completion, and submission of the cross-border personal data transfer impact assessment dossier in accordance with regulations, in respect of the violations prescribed in Clause 1 of this Article;
- b) Mandatory cessation of the cross-border personal data transfer until all dossier-related obligations have been fulfilled and confirmation has been obtained from the specialized personal data protection authority, in respect of the violations prescribed in Points a and b Clause 1 and Points a and b Clause 2 of this Article;
- c) Mandatory requirement for the cross-border data recipient to destroy or irreversibly delete all personal data transferred contrary to regulations, and provision to the competent authority of evidence that the recipient has completed such destruction or deletion, in respect of the violations prescribed in Clauses 2 and 3 of this Article;
- d) Mandatory remittance of proceeds obtained from the violations prescribed in Clause 3 of this Article.

Article 57. Violations of regulations on designation of personal data protection personnel and units

1. A warning or a fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed on an agency or organization that commits any of the following violations:

- a) Failing to enter into a confidentiality agreement with its personal data protection personnel;
- b) Failing to provide its personal data protection personnel with training and refresher training in personal data protection knowledge and skills;
- c) Issuing an official instrument designating personal data protection personnel, or a decision establishing a personal data protection unit, that fails to clearly specify its functions, duties, entitlements, and requirements concerning personal data protection activities as prescribed by law.

2. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed on an agency or organization that commits any of the following violations:

- a) Designating personal data protection personnel who do not possess a college-level or higher qualification or at least 2 years of working experience related to any of the following fields: legal

affairs, information technology, cybersecurity, data security, risk management, compliance control, or human resource management;

b) Designating personal data protection personnel who have not received training or refresher training in personal data protection law and professional personal data protection skills;

c) Failing to issue an official instrument designating personal data protection personnel, or failing to issue a decision establishing a personal data protection unit.

3. Remedial measures:

a) Mandatory replacement with personnel who fully satisfy the conditions prescribed by law, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 2 of this Article;

b) Mandatory issuance of a designation instrument, complete specification of the relevant functions and duties in accordance with regulations, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 1 of this Article.

Article 58. Violations of regulations on provision of personal data protection services

1. A fine ranging from VND 10.000.000 to VND 30.000.000 shall be imposed on an individual providing personal data protection services who commits any of the following violations:

a) Providing services despite not possessing a college-level or higher qualification or at least 3 years of working experience related to any of the following fields: legal affairs, personal data processing, cybersecurity, data security, risk management, or compliance control, or despite not having received advanced training or refresher training in personal data protection;

b) Providing services beyond the scope and duties agreed upon in the contract;

c) Failing to delete or destroy personal data processed during the provision of services after completion of the contract.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed on an organization providing personal data protection services that commits any of the following violations:

a) Failing to prepare a capability profile, or providing a capability profile that does not contain all required information;

b) Failing to have at least 3 personnel who fully satisfy the prescribed competency requirements;

c) Failing to enter into a service contract and personal data processing agreement with the agency or organization using the services before commencing the provision of services;

d) Failing to publicly disclose information concerning the service provider to data subjects and relevant parties.

3. A fine ranging from VND 50.000.000 to VND 100.000.000 shall be imposed for misusing the provision of services to access, collect, use, disclose, or process personal data beyond the contractual scope, or to commit other unlawful acts.

4. Additional penalties:

a) Confiscation of exhibits and means used for committing the administrative violation prescribed in Clause 3 of this Article;

b) Suspension of personal data protection service provision activities for a definite period of between 6 and 12 months in respect of the violations prescribed in Points a and b Clause 2 and Clause 3 of this Article.

5. Remedial measures:

a) Mandatory destruction or irreversible deletion of all personal data unlawfully collected or processed during the provision of services, in respect of the violations prescribed in Point c Clause 1 and Clause 3 of this Article;

b) Mandatory remittance of proceeds obtained from the violation prescribed in Clause 3 of this Article;

c) Mandatory notification to agencies and organizations currently using the services that the service-providing organization or individual no longer satisfies the prescribed conditions, enabling such agencies and organizations to promptly implement replacement measures to ensure the continuity of personal data protection activities, in respect of the violations prescribed in Points a and b Clause 2 of this Article.

Article 59. Violations of regulations on business provision of personal data processing services

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed on an organization conducting business in personal data processing services that has been issued a certificate and commits any of the following violations:

a) Failing to establish a personal data protection risk governance framework appropriate to the services provided;

b) Failing to establish rules on the organization's responsibilities and entitlements in personal data processing;

c) Failing to apply standards and technical regulations relating to data security, personal data protection, and cybersecurity;

d) Failing to authenticate the organization's identity in accordance with the law on electronic identification and authentication.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed on an organization conducting business in personal data processing services that has been issued a certificate and commits any of the following violations:

a) Where the organization acts as a personal data processing party, failing to require the personal data controlling party to obtain the data subject's consent before providing the services, or failing to ensure that the data subject is informed of the categories of data to be processed, the processing purposes, and the organization providing the services;

b) Failing to ensure that personal data is processed for the proper purposes; failing to appropriately limit its collection, transfer, or retention as prescribed; or failing to adopt measures to prevent unauthorized access, collection, use, or disclosure of personal data during the provision of services;

c) Failing to assess the current state of compliance and level of reliability concerning personal data protection once every year.

3. A fine ranging from VND 50.000.000 to VND 80.000.000 shall be imposed on an organization conducting business in personal data processing services that commits any of the following violations:

a) Conducting business in personal data processing services without having been issued a certificate of eligibility to conduct business in personal data processing services;

b) Assigning personal data protection personnel who do not possess a college-level or higher qualification or at least 3 years of working experience related to any of the following fields: legal affairs, personal data processing, cybersecurity, data security, risk management, or compliance control, or who have not received advanced training or refresher training in personal data protection;

c) Failing to have at least 3 personnel who satisfy the prescribed competency requirements.

4. A fine ranging from VND 80.000.000 to VND 100.000.000 shall be imposed for continuing to conduct business in personal data processing services after the certificate of eligibility to conduct business in personal data processing services has been revoked.

5. Remedial measures:

a) Mandatory establishment, promulgation, and implementation of a risk governance framework, rules on responsibilities, technical standards, and an identity authentication mechanism in accordance with regulations, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 1 of this Article;

b) Mandatory destruction or irreversible deletion of all personal data unlawfully collected or processed during the provision of services, in respect of the violations prescribed in Clauses 2 and 3 of this Article;

c) Mandatory remittance of proceeds obtained from the violations prescribed in Clause 3 of this Article.

Article 60. Violations of regulations on protection of personal data of children, persons who have lost or have limited legal capacity, and persons with difficulties in cognition or behavior control

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to perform an age-verification process before processing a child's personal data;

b) Processing the personal data of a child under 7 years of age, a person who has lost or has limited legal capacity, or a person with difficulties in cognition or behavior control without the consent of their legal representative, except in the cases prescribed in Clause 1 Article 19 of the Law on Personal Data Protection;

c) Processing the personal data of a child aged 7 years or older without obtaining the consent of both the child and their legal representative, except in the cases prescribed in Clause 1 Article 19 of the Law on Personal Data Protection.

2. A fine ranging from VND 50.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

a) Processing the personal data of a child for the purpose of publicly disclosing or revealing information concerning the private life or personal secrets of a child aged 7 years or older without obtaining the consent of both the child and their legal representative;

b) Failing to cease processing the personal data of a child, a person who has lost or has limited legal capacity, or a person with difficulties in cognition or behavior control when their legal representative withdraws consent, unless otherwise prescribed by law;

c) Failing to cease processing the personal data of a child, a person who has lost or has limited legal capacity, or a person with difficulties in cognition or behavior control when a competent authority has sufficient grounds to demonstrate that the data processing may infringe upon the lawful rights and interests of the protected person and requests cessation of the processing, unless otherwise prescribed by law.

3. A fine ranging from VND 100.000.000 to VND 200.000.000 shall be imposed for failing to irreversibly delete or destroy a child's personal data where the data has been processed for improper purposes, or the processing purposes have been fulfilled; the child's parent or guardian has withdrawn consent; or a competent authority has requested such deletion or destruction.

4. Additional penalty: Suspension of the personal data processing activities directly related to the violation for a definite period of between 1 and 3 months in respect of the violations prescribed in Clause 2 of this Article, or between 3 and 6 months in respect of the violation prescribed in Clause 3 of this Article.

5. Remedial measures:

a) Mandatory cessation of personal data processing activities and written notification to the legal representative of such cessation, in respect of the violations prescribed in Points b and c Clause 2 of this Article;

b) Mandatory destruction or irreversible deletion of all personal data processed contrary to regulations, in respect of the violations prescribed in Clauses 1, 2, and 3 of this Article;

c) Mandatory removal of unlawfully disclosed information concerning private life or personal secrets and notification to the legal representative of such removal, in respect of the violation prescribed in Point a Clause 2 of this Article.

Article 61. Violations of regulations on personal data protection in recruitment, management, and use of employees

1. A fine ranging from VND 20.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Requiring an applicant to provide personal data that does not serve recruitment purposes or is inconsistent with the law;

b) Using an applicant's personal data for purposes other than recruitment without an agreement with the applicant;

c) Processing an applicant's personal data without consent or beyond the scope or purposes to which the applicant has consented;

d) Failing to delete or destroy an applicant's personal data where the applicant is not recruited, unless otherwise agreed with the applicant.

2. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Retaining an employee's personal data beyond the period prescribed by law or the agreed period;

b) Failing to delete or destroy an employee's personal data upon termination of the employment contract, unless otherwise agreed or prescribed by law;

c) Applying technological or technical measures to collect an employee's personal data without ensuring that the employee is fully informed of such measures, including installing device-monitoring software, surveillance cameras, or other data-collection devices in the workplace without notifying the employee;

d) Applying technological or technical measures to collect an employee's personal data inconsistently with the law or without ensuring the employee's lawful rights and interests.

3. A fine ranging from VND 70.000.000 to VND 100.000.000 shall be imposed for processing or using an employee's personal data collected through technological or technical measures contrary to the law.

4. Remedial measures:

a) Mandatory destruction or irreversible deletion of personal data collected or processed contrary to regulations, in respect of the violations prescribed in Points c and d Clause 1, Points c and d Clause 2, and Clause 3 of this Article;

b) Mandatory remittance of proceeds obtained from the violation prescribed in Clause 3 of this Article.

Article 62. Violations of regulations on protection of personal data relating to health information and in insurance business activities

1. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) In the course of conducting insurance, reinsurance, or reinsurance cession business, transferring a customer's personal data to a business partner without clearly and transparently providing for such transfer in the contract concluded with the client;

b) In the course of developing or operating healthcare applications or online healthcare platforms, collecting sensitive personal data without establishing rules on access authorization and restrictions or implementing prescribed security measures.

2. A fine ranging from VND 70.000.000 to VND 100.000.000 shall be imposed for providing or sharing a patient's personal data with a third party that is another healthcare service provider or an enterprise conducting health insurance or life insurance business without receiving a written request from the data subject.

3. Additional penalty: Suspension of the personal data processing activities directly related to the violation for a definite period of between 1 and 3 months in respect of the violations prescribed in Clause 1 of this Article, or between 3 and 6 months in respect of the violation prescribed in Clause 2 of this Article.

4. Remedial measures:

a) Mandatory establishment and implementation of security and access authorization measures in accordance with applicable technical regulations for systems collecting health and biometric data, and provision of evidence of implementation to the competent authority, in respect of the violation prescribed in Point b Clause 1 of this Article;

b) Mandatory requirement for the third party to destroy or irreversibly delete all personal data unlawfully received, and provision to the competent authority of evidence of such destruction or deletion, in respect of the violation prescribed in Clause 2 of this Article;

c) Mandatory remittance of illegal proceeds obtained from the violation prescribed in Clause 2 of this Article.

Article 63. Violations of regulations on personal data protection in advertising service business

1. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Collecting and using basic personal data to deliver advertisements without the data subject's consent;

b) An organization or individual conducting the advertising service business failing to provide a transparent and readily accessible technical mechanism or method through which the data subject may exercise the right to opt out of advertisements or withdraw consent to the sharing of personal data for advertising purposes;

c) Establishing consent by default to the provision of a data subject's personal data to an affiliated advertising network;

d) Deliberately sharing a user profile with a third party for advertising service business purposes after the user has opted out.

2. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Collecting and using sensitive personal data to deliver advertisements without the data subject's consent;

b) Conducting advertising service business based on the personal data of a child under 16 years of age without the consent of their legal representative;

c) Collecting personal data by tracking websites, web portals, or applications for behavioral or targeted advertising or for the personalization of advertisements without the data subject's consent;

d) Failing to establish a method through which the data subject may refuse the sharing of personal data for behavioral or targeted advertising or for the personalization of advertisements;

dd) Deliberately retaining, or failing to delete or destroy, personal data that is no longer necessary for the processing purposes as prescribed by law.

3. Additional penalty: Suspension of advertising service provision activities directly related to the violation for a definite period of between 1 and 3 months in respect of the violations prescribed in Clause 1, or between 3 and 6 months in respect of the violations prescribed in Clause 2 of this Article.

4. Remedial measures:

a) Mandatory destruction or irreversible deletion of personal data unlawfully collected or used to deliver advertisements, in respect of the violations prescribed in Clauses 1 and 2 of this Article;

b) Mandatory remittance of proceeds obtained from the violations prescribed in Clauses 1 and 2 of this Article;

c) Mandatory establishment and provision to users of a mechanism for opting out of advertisements and withdrawing consent to data sharing in accordance with regulations, and provision of evidence of implementation to the competent authority, in respect of the violation prescribed in Point b Clause 1 of this Article.

Article 64. Violations of regulations on personal data protection in financial, banking, and credit information activities

1. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Failing to notify, or notifying more than 72 hours after detecting an incident involving the disclosure or loss of sensitive personal data, the specialized personal data protection authority and the data subject of such incident;

b) Providing notification of a personal data protection incident that does not contain all minimum information prescribed by law;

c) Failing to keep logs of all personal data processing activities, or failing to conduct an annual compliance assessment as prescribed;

d) Failing to establish a solution for recovering personal data in the event of a data loss incident;

dd) Failing to apply prescribed standards and technical regulations on personal data protection, personal data de-identification, and personal data anonymization;

e) Obtaining the data subject's consent without clearly stating the information prescribed in Clause 2 Article 9 of the Law on Personal Data Protection.

2. A fine ranging from VND 70.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

a) Using a data subject's personal data to conduct credit scoring, credit rating, or creditworthiness assessments without the data subject's consent, except where personal data may be processed without the data subject's consent;

b) An organization conducting credit information activities failing to implement managerial and technical measures to prevent and combat unauthorized access, use, disclosure, or modification of clients' personal data;

c) Collecting personal data beyond the scope necessary for credit information activities, or collecting such data from sources not permitted by law.

3. Additional penalty: Suspension of the provision of credit information, credit scoring, credit rating, or creditworthiness assessment services for a definite period of between 1 and 3 months in respect of the violations prescribed in Clause 1, or between 3 and 6 months in respect of the violations prescribed in Clause 2 of this Article.

4. Remedial measures:

a) Mandatory destruction or irreversible deletion of unlawfully generated credit scoring or credit rating results, in respect of the violation prescribed in Point a Clause 2 of this Article;

b) Mandatory requirement for partners and affiliated parties to destroy or irreversibly delete sensitive personal data unlawfully shared or transferred to them, in respect of the violation prescribed in Point b Clause 2 of this Article.

Article 65. Violations of regulations on personal data protection applicable to social networking platforms and online communication services

1. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed on an organization providing social networking services, online communication services, or a digital content platform that commits any of the following violations:

a) Failing to clearly notify the data subject of the categories of personal data collected when the data subject installs and uses the social network or online communication service;

b) Failing to provide an option allowing users to refuse the collection and sharing of data files known as cookies;

c) Failing to provide a "do not track" option, or tracking users' activities on a social network or online communication service without their consent;

d) Failing to transparently publish a privacy policy, or failing to provide a clear and comprehensible explanation of how personal data is collected, used, retained, and shared;

dd) Failing to provide users with mechanisms to access, rectify, or delete their personal data; configure privacy settings for their personal accounts; or report privacy and confidentiality violations;

e) Failing to clearly notify the data subject of the categories of personal data to be collected when the data subject installs and uses an application.

2. A fine ranging from VND 70.000.000 to VND 150.000.000 shall be imposed for any of the following violations:

a) Requiring a user to provide an image or video containing all or part of an identification document as a mandatory condition for authenticating an ordinary user account where identification is not required by specialized law;

b) An OTT application or social network using undisclosed technological features to eavesdrop on or record calls, read text messages, or automatically extract contacts or media files from a device without the data subject's consent, unless otherwise prescribed by law;

c) Unlawfully collecting personal data beyond the scope agreed upon with the user when the service was installed.

3. Additional penalty: Suspension of service provision activities of the relevant application or digital platform in Vietnam for a definite period of between 1 and 3 months in respect of the violations prescribed in Clause 1, or between 3 and 6 months in respect of the violations prescribed in Clause 2 of this Article.

4. Remedial measures:

a) Mandatory establishment and provision to users of features allowing them to refuse tracking and the sharing of cookies, and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Points b and c Clause 1 of this Article;

b) Mandatory destruction or irreversible deletion of personal data, identification documents, contacts, or files unlawfully collected or extracted, in respect of the violations prescribed in Clause 2 of this Article.

Article 66. Violations of regulations on personal data protection in big data processing

1. A fine ranging from VND 20.000.000 to VND 30.000.000 shall be imposed for any of the following violations:

a) Processing big data containing personal data without establishing appropriate policies on the retention, deletion, and destruction of personal data in accordance with the law;

b) Failing to enter into written agreements with third parties, partners, and service providers to ensure full compliance with personal data protection regulations;

c) Failing to periodically provide training, disseminate information, and raise personnel awareness concerning personal data confidentiality, particularly among personnel directly involved in data processing.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Failing to establish a notification mechanism or provide an appropriate explanation to the data subject that their data has been incorporated into a big data analytics system;

b) Failing to use strong authentication methods, which must include at least multi-factor authentication, or failing to implement access authorization to ensure that only authorized persons may access the data;

c) Failing to conduct continuous monitoring or use monitoring tools to track access activities and detect unusual activities;

d) Failing to conduct periodic cybersecurity and data security inspections and assessments to detect, prevent, and remediate security vulnerabilities;

dd) Failing to encrypt and anonymize personal data during its transfer or provision, unless otherwise prescribed by specialized law.

3. A fine ranging from VND 50.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

a) Operating a big data system that makes automated decisions affecting security and order or the lawful rights and interests of organizations or individuals without establishing an oversight mechanism or allowing a request for human review;

b) Using or developing a big data system that processes personal data for the purpose of causing harm to security and order or infringing upon the honor, dignity, or property of another individual.

4. Additional penalties:

a) Confiscation of exhibits and means directly used for committing the administrative violations prescribed in Clauses 2 and 3 of this Article;

b) Suspension of the operation of systems, platforms, or applications performing big data analytics involving personal data processing for a definite period of between 3 and 6 months in respect of the violations prescribed in Clause 3 of this Article.

5. Remedial measures:

- a) Mandatory establishment, promulgation, and publication of policies on the retention, deletion, and destruction of personal data and organizational personal data protection measures in accordance with the law; mandatory supplementation or revision of agreements with third parties, partners, and service providers to ensure compliance with personal data protection regulations; and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 1 of this Article;
- b) Mandatory implementation of appropriate technical and organizational security measures, including multi-factor authentication, access authorization, encryption, and personal data anonymization during data transfer and provision; mandatory provision of complete and transparent information to the data subject concerning the incorporation of their data into a big data analytics system; and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 2 of this Article;
- c) Mandatory cessation of personal data processing activities conducted contrary to regulations until the violation has been remedied and confirmation has been obtained from the competent authority; mandatory destruction or irreversible deletion of unlawfully processed personal data; and mandatory full fulfillment of data subject rights, including the right to request human review of an automated decision;
- d) Mandatory remittance of proceeds obtained from the violations prescribed in Clause 3 of this Article.

Article 67. Violations of regulations on personal data protection in artificial intelligence systems and metaverse

- 1. A fine ranging from VND 20.000.000 to VND 50.000.000 shall be imposed for processing personal data in an artificial intelligence system or a metaverse without conducting an annual assessment of compliance with personal data protection regulations.
- 2. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:
 - a) Failing to notify or explain to the data subject the operating principles of an automated algorithm and its effects on the data subject's lawful rights and interests;
 - b) Failing to provide tools or mechanisms through which the data subject may exercise the right to opt out of automated data processing;
 - c) Failing to ensure the data subject's rights to rectify, anonymize, or delete their identification profile;
 - d) Failing to classify artificial intelligence systems by risk level for the establishment of appropriate personal data protection measures;

dd) Failing to implement personal data protection measures when using artificial intelligence inference outputs to identify or assist in identifying a specific individual;

e) Developing or deploying an artificial intelligence system or a metaverse without building a system that meets cybersecurity and comprehensive data protection standards, or without establishing a system for monitoring and providing early warnings of cybersecurity risks;

g) Failing to apply appropriate authentication and identification methods, or failing to implement access authorization for personal data processing within the system.

3. A fine ranging from VND 70.000.000 to VND 100.000.000 shall be imposed for any of the following violations:

a) Failing to establish mechanisms to control and prevent the misuse of artificial intelligence or the metaverse for activities infringing upon national security or social order and safety;

b) Developing or operating an artificial intelligence system or a metaverse that makes automated decisions affecting security and order or the lawful rights and interests of organizations or individuals without establishing an oversight mechanism or allowing requests for human review;

c) Using or developing an artificial intelligence system or a metaverse for the purpose of causing harm to security and order or infringing upon the honor, dignity, or property of another individual.

4. Additional penalties:

a) Confiscation of exhibits and means directly used for committing the administrative violations prescribed in Clauses 2 and 3 of this Article;

b) Suspension of the operation of artificial intelligence or metaverse systems, platforms, or applications involving personal data processing for a definite period of between 3 and 6 months in respect of the violations prescribed in Clause 3 of this Article.

5. Remedial measures:

a) Mandatory establishment, promulgation, and full implementation of mechanisms for notifying and explaining to data subjects the operating principles of algorithms; mandatory provision of tools and mechanisms through which data subjects may exercise the right to opt out of automated processing and the rights to rectify, anonymize, and delete identification profiles; mandatory implementation of appropriate technical and organizational security measures, including risk classification, identity authentication, access authorization, and protection of inference outputs that identify individuals; and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 2 of this Article;

b) Mandatory cessation of personal data processing activities conducted contrary to regulations until the violation has been remedied and confirmation has been obtained from the competent

authority; mandatory destruction or irreversible deletion of unlawfully processed personal data; and mandatory full fulfillment of data subject rights, including the right to request human review of an automated decision;

c) Mandatory remittance of proceeds obtained from the violations prescribed in Clause 3 of this Article.

Article 68. Violations of regulations on personal data protection in blockchain technology

1. A fine ranging from VND 20.000.000 to VND 50.000.000 shall be imposed for processing personal data using blockchain technology without conducting an annual assessment of compliance with personal data protection regulations.

2. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Failing to apply encryption, hashing, and digital signature algorithms that ensure security when processing personal data on a blockchain;

b) Failing to apply appropriate authentication and identification methods, or failing to implement access authorization for personal data processing.

3. A fine ranging from VND 70.000.000 to VND 150.000.000 shall be imposed for using blockchain technology to directly store personal data in plaintext on a blockchain network without performing de-identification procedures or applying data-hashing algorithms.

4. Additional penalties:

a) Confiscation of exhibits and means directly used for committing the administrative violations prescribed in Clauses 2 and 3 of this Article;

b) Suspension of the operation of blockchain systems, platforms, or applications involving personal data processing for a definite period of between 3 and 6 months in respect of the violation prescribed in Clause 3 of this Article.

5. Remedial measures:

a) Mandatory implementation of appropriate technical and organizational security measures, including secure encryption, hashing and digital signature algorithms; establishment of identity authentication methods and access authorization in accordance with regulations; and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 2 of this Article;

b) Mandatory cessation of the storage of personal data in plaintext on the blockchain network until the violation has been remedied and confirmation has been obtained from the competent authority;

c) Mandatory implementation of technical measures to remove personal data unlawfully stored in its original form on the blockchain to the extent that the relevant individuals can no longer be identified;

d) Mandatory remittance of proceeds obtained from the violations prescribed in Clause 3 of this Article.

Article 69. Violations of regulations on personal data protection in cloud computing

1. A fine ranging from VND 20.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

a) Providing cloud computing services without providing partners and relevant parties with information concerning the personal data protection unit and personnel;

b) An organization using cloud computing services failing to clearly determine the personal data processing flows and the roles and responsibilities of the parties in its contract with the service provider, or failing to include requirements for technical and organizational security measures in the contract;

c) A cloud computing service provider failing to require and contractually bind its subcontractors to comply with personal data protection regulations and obligations;

d) Failing to establish appropriate policies on the retention, deletion, and destruction of personal data;

dd) An organization providing cloud computing services failing to conduct an annual assessment of compliance with personal data protection regulations.

2. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Providing or using cloud computing services without implementing technical and organizational measures to prevent unauthorized access to personal data;

b) Providing or using cloud computing services without encrypting clients' personal data at rest and in transit;

c) Failing to apply appropriate authentication and identification methods, or failing to implement strict access authorization for personal data processing in a cloud computing environment;

d) An organization using cloud computing services failing to notify relevant parties of changes to systems or infrastructure that may affect personal data security.

3. A fine ranging from VND 70.000.000 to VND 100.000.000 shall be imposed for using or developing a cloud computing system for the purpose of causing harm to security and order or infringing upon the honor, dignity, or property of another individual.

4. Additional penalties:

a) Confiscation of exhibits and means directly used for committing the administrative violations prescribed in Clauses 2 and 3 of this Article;

b) Suspension of the operation of cloud computing systems, platforms, or applications involving personal data processing for a definite period of between 3 and 6 months in respect of the violation prescribed in Clause 3 of this Article.

5. Remedial measures:

a) Mandatory establishment, promulgation, and publication of policies on the retention, deletion, and destruction of personal data in accordance with the law; mandatory supplementation or revision of contracts with cloud computing service providers and requirement for subcontractors to fully comply with personal data protection regulations and obligations; and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 1 of this Article;

b) Mandatory implementation of appropriate technical and organizational security measures, including encryption of personal data at rest and in transit, identity authentication, strict access authorization, and measures to prevent unauthorized access; and provision of evidence of implementation to the competent authority, in respect of the violations prescribed in Clause 2 of this Article;

c) Mandatory cessation of personal data processing activities conducted contrary to regulations until the violation has been remedied and confirmation has been obtained from the competent authority, and mandatory destruction or irreversible deletion of unlawfully processed personal data;

d) Mandatory remittance of proceeds obtained from the violation prescribed in Clause 3 of this Article.

Article 70. Violations of regulations on protection of personal location data and biometric data

1. A fine ranging from VND 50.000.000 to VND 70.000.000 shall be imposed for any of the following violations:

a) Providing a platform or mobile application that collects personal location data without notifying users of the use of such data;

- b) Failing to implement technical measures to prevent unrelated third parties from collecting personal location data, or failing to provide users with options for controlling personal location tracking;
- c) Collecting or processing biometric data without establishing physical security measures for systems and devices used to retain and transmit such data;
- d) Failing to restrict access rights or establish a monitoring system to prevent infringements involving personal location data or biometric data;
- dd) Failing to notify the specialized personal data protection authority and affected data subjects within 72 hours after detecting a personal data breach involving location data or biometric data;
- e) Providing affected data subjects with a notification that does not contain the minimum information prescribed by law;
- g) Failing to record, retain, and update violation dossiers for inspection, examination, and handling purposes, or failing to retain such dossiers for at least 5 years from the date on which the incident has been completely remedied;
- h) Where it is impossible to notify all affected data subjects within the prescribed period for technical reasons or due to an emergency, failing to issue a public notification through the organization's official electronic means, including its website or application, or failing to send notifications to relevant data subjects where technically possible.

2. A fine ranging from VND 70.000.000 to VND 150.000.000 shall be imposed for any of the following violations:

- a) Installing or using location-tracking technologies through radio-frequency identification tags or other technologies without the data subject's consent or a request from a competent authority as prescribed by law, unless otherwise prescribed by law;
- b) Utilizing or using a data subject's biometric data beyond the original purposes without obtaining consent.

3. Additional penalties:

- a) Confiscation of transmitting devices, RFID tags, data-collection devices, and biometric data storage servers used for committing the violations prescribed in Clause 2 of this Article;
- b) Suspension of the operation of location-tracking systems, platforms, or applications involving personal data processing for a definite period of between 3 and 6 months in respect of the violations prescribed in Clause 2 of this Article.

4. Remedial measures:

- a) Mandatory destruction or irreversible deletion of personal location data and biometric data unlawfully collected or tracked, in respect of the violations prescribed in Clause 2 of this Article;
- b) Mandatory provision to users of an option to enable or disable the collection of personal location data, and provision of evidence of implementation to the competent authority, in respect of the violation prescribed in Point b Clause 1 of this Article.

Article 71. Violations of regulations on protection of personal data obtained from audio and video recording activities in public places

1. A fine ranging from VND 10.000.000 to VND 20.000.000 shall be imposed for any of the following violations:

- a) Installing or using audio or video recording equipment in public spaces or customer service areas without providing notice or warnings through physical signs or electronic means placed in a conspicuous location, enabling data subjects to understand that they are being recorded;
- b) Failing to provide the contact information of the personal data controlling party or the personal data processing and controlling party when a data subject requests access to images of themselves, unless otherwise prescribed by law.

2. A fine ranging from VND 30.000.000 to VND 50.000.000 shall be imposed for any of the following violations:

- a) Using personal data, images, or voice recordings obtained from a public surveillance camera system for commercial purposes, behavioral analysis, or automated facial recognition to create personal profiles without the data subject's lawful consent;
- b) Unlawfully extracting, sharing, or publicly disclosing audio or video recordings, except where such recordings are provided in response to a written request from a competent authority.

3. Additional penalty: Confiscation of exhibits and means used for committing the administrative violations prescribed in Clause 2 of this Article.

4. Remedial measures:

- a) Mandatory destruction or irreversible deletion of audio and image data collected contrary to regulations, in respect of the violations prescribed in Clauses 1 and 2 of this Article;
- b) Mandatory establishment and publication of the contact information of the personal data controlling party, enabling data subjects to request access to images of themselves, and provision of evidence of implementation to the competent authority, in respect of the violation prescribed in Point b Clause 1 of this Article.

Chapter III

COMPETENCE TO MAKE ADMINISTRATIVE VIOLATION RECORDS AND IMPOSE PENALTIES FOR ADMINISTRATIVE VIOLATIONS

Article 72. Competence of People's Public Security Force to impose penalties for administrative violations

1. A People's Public Security officer on duty has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 20.000.000 for administrative violations in the field of cybersecurity and up to 10% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause.

2. The Head of a commune-level Police Authority has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 100.000.000 for administrative violations in the field of cybersecurity and up to 50% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

3. Heads of professional divisions under the Department of Foreign Security, Department of Internal Security, Department of Internal Political Security, Department of Economic Security, Department of Cybersecurity and High-Tech Crime Prevention and Control, Immigration Department, Office of the Investigation Police Agency, Department of Police Investigation of Crimes against Social Order, Police Department for Administrative Management of Social Order, Department of Police Investigation of Crimes of Corruption, Economy, and Smuggling, and National Data Center; and heads of the following divisions under provincial-level Police Authorities: Head of the Foreign Security Division, Head of the Internal Security Division, Head of the Internal Political Security Division, Head of the Economic Security Division, Head of the Cybersecurity and High-Tech Crime Prevention and Control Division, Chief of the Office of the Investigation Police Agency, Head of the Division of Police Investigation of Crimes against Social Order, Head of the Division of Police Investigation of Crimes of Corruption, Economy, and Smuggling, Head of the Police Division for Administrative Management of Social Order, and Head of the Criminal Police Division, have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 160.000.000 for administrative violations in the field of cybersecurity and up to 80% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

4. The Head of the Immigration Division of a provincial-level Police Authority has the sanctioning competence prescribed in Clause 3 of this Article and the power to impose expulsion as a penalty.

5. The Director of a provincial-level Police Authority has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 200.000.000 for administrative violations in the field of cybersecurity and up to the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations;
- dd) Impose expulsion as a penalty;
- e) Apply the remedial measures prescribed in Article 5 of this Decree.

6. The Director of the Department of Foreign Security; Director of the Department of Internal Security; Director of the Department of Internal Political Security; Director of the Department of Economic Security; Director of the Department of Cybersecurity and High-Tech Crime Prevention and Control; Chief of the Office of the Investigation Police Agency; Director of the Department of Police Investigation of Crimes against Social Order; Director of the Department of Police Investigation of Crimes of Corruption, Economy, and Smuggling; Director of the Police Department for Administrative Management of Social Order; Director of the Criminal Police Department; and Director of the National Data Center have the power to:

- a) Issue warnings;

b) Impose fines of up to VND 200.000.000 for administrative violations in the field of cybersecurity and up to the maximum fine applicable to the field of personal data protection prescribed in Chapter II;

c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;

d) Confiscate exhibits and means of administrative violations;

dd) Apply the remedial measures prescribed in Article 5 of this Decree.

7. The Director of the Immigration Department has the sanctioning competence prescribed in Clause 6 of this Article and the power to impose expulsion as a penalty.

Article 73. Competence of Presidents of People's Committees at all levels to impose penalties for administrative violations

1. The President of a commune-level People's Committee has the power to:

a) Issue warnings;

b) Impose fines of up to VND 100.000.000 for administrative violations in the field of cybersecurity and up to 50% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;

c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;

d) Confiscate exhibits and means of administrative violations;

dd) Apply the remedial measures prescribed in Article 5 of this Decree.

2. The President of a provincial People's Committee has the power to:

a) Issue warnings;

b) Impose fines of up to VND 200.000.000 for administrative violations in the field of cybersecurity and up to the maximum fine applicable to the field of personal data protection prescribed in Chapter II;

c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;

d) Confiscate exhibits and means of administrative violations;

dd) Apply the remedial measures prescribed in Article 5 of this Decree.

Article 74. Competence of inspectorates to impose administrative penalties

1. Inspectors of the Ministry of National Defense of Vietnam and the Ministry of Public Security of Vietnam have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 20.000.000 for administrative violations in the field of cybersecurity and up to 10% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause.

2. Heads of inspection teams of military zones, the Hanoi Capital Command, and provincial-level Police Authorities have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 100.000.000 for administrative violations in the field of cybersecurity and up to 50% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause.

3. Chief Defense Inspectors of military zones, the Chief Defense Inspector of the Hanoi Capital Command, and Chief Inspectors of provincial-level Police Authorities assigned to perform inspection and examination duties within the scope of state management of a ministry or ministerial agency have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 160.000.000 for administrative violations in the field of cybersecurity and up to 80% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

4. The Chief Inspectors of the Ministry of National Defense of Vietnam, the Ministry of Public Security of Vietnam, and the State Bank of Vietnam, and heads of inspection teams established

by the Chief Inspector of the Ministry of National Defense of Vietnam or the Chief Inspector of the Ministry of Public Security of Vietnam, have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 200.000.000 for administrative violations in the field of cybersecurity and up to the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

Article 75. Competence of Border Guard to impose administrative penalties

1. A Border Guard soldier on duty has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 10.000.000 for administrative violations in the field of cybersecurity and up to 5% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause.

2. Heads of Border Guard Stations and Teams have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 20.000.000 for administrative violations in the field of cybersecurity and up to 10% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause;
- d) Apply the remedial measures prescribed in Points a and c Clause 1 of Article 28 of the Law on Handling of Administrative Violations.

3. The Head of a Special Task Team for Drug and Crime Prevention and Control under a Special Task Force for Drug and Crime Prevention and Control has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 30.000.000 for administrative violations in the field of cybersecurity and up to 15% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause;
- d) Apply the remedial measures prescribed in Points a and e Clause 1 of Article 28 of the Law on Handling of Administrative Violations.

4. Chiefs of Border Guard Posts, Commanders of Border Guard Squadrons, and Commanders of Port Border Checkpoint Border Guard Commands have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 60.000.000 for administrative violations in the field of cybersecurity and up to 30% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause;
- d) Apply the remedial measures prescribed in Article 5 of this Decree.

5. The Commander of a Special Task Force for Drug and Crime Prevention and Control under the Department of Drug and Crime Prevention and Control of the Border Guard High Command has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 100.000.000 for administrative violations in the field of cybersecurity and up to 50% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

6. Commanders of Border Guard Commands; Commanders of Border Guard Flotillas; and the Director of the Department of Drug and Crime Prevention and Control under the Border Guard High Command have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 200.000.000 for administrative violations in the field of cybersecurity and up to the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

Article 76. Competence of Coast Guard to impose administrative penalties

1. A Coast Guard officer on duty has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 10.000.000 for administrative violations in the field of cybersecurity and up to 5% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause.

2. The Head of a Coast Guard Professional Team has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 20.000.000 for administrative violations in the field of cybersecurity and up to 10% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause.

3. Heads of Coast Guard Professional Teams and Heads of Coast Guard Stations have the power to:

- a) Issue warnings;

b) Impose fines of up to VND 40.000.000 for administrative violations in the field of cybersecurity and up to 20% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;

c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause;

d) Apply the remedial measures prescribed in Points a and e Clause 1 of Article 28 of the Law on Handling of Administrative Violations.

4. Commanders of Coast Guard Squadrons have the power to:

a) Issue warnings;

b) Impose fines of up to VND 60.000.000 for administrative violations in the field of cybersecurity and up to 30% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;

c) Confiscate exhibits and means of administrative violations whose value does not exceed twice the fine specified in Point b of this Clause;

d) Apply the remedial measures prescribed in Article 5 of this Decree.

5. Commanders of Coast Guard Flotillas, Commanders of Reconnaissance Units, and Commanders of Special Task Units for Drug Crime Prevention and Control under the Vietnam Coast Guard have the power to:

a) Issue warnings;

b) Impose fines of up to VND 100.000.000 for administrative violations in the field of cybersecurity and up to 50% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;

c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;

d) Confiscate exhibits and means of administrative violations;

dd) Apply the remedial measures prescribed in Article 5 of this Decree.

6. Commanders of Coast Guard Regional Commands and the Director of the Department of Professional Operations and Legal Affairs under the Vietnam Coast Guard have the power to:

a) Issue warnings;

- b) Impose fines of up to VND 160.000.000 for administrative violations in the field of cybersecurity and up to 80% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

7. The Commander of the Vietnam Coast Guard has the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 200.000.000 for administrative violations in the field of cybersecurity and up to the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

Article 77. Competence of agencies performing state management duties in specialized sectors and fields and of certain other title holders

1. Directors of Departments of Culture, Sports and Tourism; Directors of Departments of Science and Technology; Directors of Departments of Industry and Trade; and heads of inspection teams established by the Director of the Authority of Broadcasting and Electronic Information have the power to:

- a) Issue warnings;
- b) Impose fines of up to VND 160.000.000 for administrative violations in the field of cybersecurity and up to 80% of the maximum fine applicable to the field of personal data protection prescribed in Chapter II;
- c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;
- d) Confiscate exhibits and means of administrative violations;
- dd) Apply the remedial measures prescribed in Article 5 of this Decree.

2. The Chief of Office of the Ministry of Science and Technology of Vietnam; heads of inspection teams established by the Minister of Science and Technology of Vietnam; the Chief of Office of the Ministry of Culture, Sports and Tourism of Vietnam; the Chief of Office of the Ministry of Industry and Trade of Vietnam; the Director of the Telecommunications Authority; the Director of the E-Commerce and Digital Economy Agency; the Director of the Press Authority; and the Director of the Authority of Broadcasting and Electronic Information have the power to:

a) Issue warnings;

b) Impose fines of up to VND 200.000.000 for administrative violations in the field of cybersecurity and up to the maximum fine applicable to the field of personal data protection prescribed in Chapter II;

c) Deprive the right to use licenses for a definite period or suspend operations for a definite period;

d) Confiscate exhibits and means of administrative violations;

dd) Apply the remedial measures prescribed in Article 5 of this Decree.

Article 78. Delineation of sanctioning competence

1. Persons of the People's Public Security Force competent to impose penalties may impose penalties for administrative violations and apply remedial measures in respect of the administrative violations prescribed in Chapter II of this Decree, within the competence prescribed in Articles 72 and 74 of this Decree and according to their assigned functions, duties, and entitlements within the fields and geographical areas under their management.

2. Chairpersons of People's Committees at all levels may impose penalties for administrative violations and apply remedial measures in respect of the administrative violations prescribed in Chapter II of this Decree, within the competence prescribed in Article 73 of this Decree and according to their assigned functions, duties, and entitlements within the fields and geographical areas under their management.

3. The National Defense Inspectorate, Inspectorate of the State Bank of Vietnam, Border Guard High Command, and Coast Guard Command may impose penalties for administrative violations and apply remedial measures in respect of the administrative violations prescribed in Chapter II of this Decree, within the scope of their assigned duties and official functions, the competence prescribed in Articles 74, 75, and 76 of this Decree, and their assigned functions, duties, and entitlements within the fields and geographical areas under their management.

4. Heads of agencies performing state management duties in specialized sectors and fields may impose penalties for administrative violations and apply remedial measures in respect of the administrative violations prescribed in Chapter II of this Decree, within the competence

prescribed in Article 77 of this Decree and according to their assigned functions, duties, and entitlements within the fields and geographical areas under their management.

Article 79. Competence to make administrative violation records

1. Persons competent to impose penalties for administrative violations as prescribed in Articles 72, 73, 74, 75, 76, and 77 of this Decree have the competence to make administrative violation records.
2. Inspectors performing inspection functions in the fields falling within the scope of regulation of this Decree; and civil servants, public employees, and members of the People's Army, People's Public Security Force, or agencies performing state management duties prescribed in Article 77 of this Decree who are performing official duties or assigned tasks in the fields of cybersecurity and personal data protection have the competence to make administrative violation records in respect of administrative violations within their assigned functions, duties, and entitlements.

Chapter IV

IMPLEMENTATION PROVISIONS

Article 80. Entry into force

This Decree comes into force as of August 19, 2026.

Article 81. Transitional provisions

1. For an administrative violation in the fields of cybersecurity or personal data protection that occurred before the effective date of this Decree but is subsequently discovered or remains under consideration or resolution, specific decrees of the Government of Vietnam prescribing penalties for administrative violations in force when the violation was committed shall apply. Where this Decree does not prescribe legal liability for such violation or prescribes less severe legal liability, this Decree shall apply.
2. Where an administrative violation record was made before the effective date of Decree but no penalty decision has been issued, the matter shall be handled as follows:
 - a) If the time limit for issuing a penalty decision has not expired, the imposition of penalties and application of remedial measures shall comply with the principle prescribed in Clause 1 of this Article;
 - b) If the prescriptive period for imposing penalties for administrative violations or the time limit for issuing a penalty decision has expired as prescribed in Point c Clause 1 of Article 65 of the Law on Handling of Administrative Violations, no penalty decision shall be issued. However, the competent person shall issue a decision on the confiscation of exhibits and means of administrative violations where such exhibits or means are prohibited from being possessed or

circulated, or where the law prescribes confiscation as a penalty for such exhibits or means, and shall apply the remedial measures prescribed for the relevant administrative violation. The confiscation of exhibits and means of administrative violations and the application of remedial measures shall comply with the principle prescribed in Clause 1 of this Article.

3. A decision on penalties for administrative violations issued before the effective date of this Decree that has not yet been fully enforced shall continue to be enforced in accordance with the issued decision.

4. Where a decision on penalties for administrative violations was issued or fully enforced before the effective date of this Decree, but the sanctioned individual or organization has an outstanding complaint, the complaint shall be resolved in accordance with the Law on Handling of Administrative Violations, specific decrees of the Government of Vietnam prescribing penalties for administrative violations, and relevant legislative documents in force when the penalty decision was issued.

5. Sanctioning competence in transitional cases shall be determined as follows:

a) Where, before the effective date of this Decree, an administrative violation case had been accepted and was being resolved by a competent person, and that person remains competent to impose penalties under this Decree, that person shall continue to resolve the case. Where the person handling the case is no longer competent, or the case exceeds that person's sanctioning competence under this Decree, the case file shall be transferred to a person competent to impose penalties under this Decree for resolution. Administrative violation records, verification results, documents, and evidence lawfully made or collected before the effective date of this Decree shall remain legally valid;

b) Where the name, functions, duties, or entitlements of an authority or title holder competent to impose penalties under this Decree are changed due to organizational restructuring, the authority or title holder succeeding to the corresponding functions, duties, and entitlements shall exercise the sanctioning competence prescribed in this Decree.

Article 82. Implementation responsibilities

1. The Minister of Public Security of Vietnam shall monitor, provide guidance on, and organize the implementation of this Decree.

2. Ministers, Directors of ministerial agencies, Presidents of People's Committees of provinces and centrally affiliated cities, and relevant organizations and individuals shall implement this Decree.

**ON BEHALF OF THE GOVERNMENT
PP. PRIME MINISTER
DEPUTY PRIME MINISTER**

Pham Gia Tuc

*This translation is made by **THƯ VIỆN PHÁP LUẬT**, Ho Chi Minh City, Vietnam and for reference purposes only. Its copyright is owned by **THƯ VIỆN PHÁP LUẬT** and protected under Clause 2, Article 14 of the Law on Intellectual Property. Your comments are always welcomed*